PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-084271
(43)Date of publication of application : 22.03.2002

(51)Int.Cl. H04L 9/08
G11B 20/10

(21)App ication number : 2000-270919
(22)Date of filing : 07.09.2000

(71)Applicant : SONY CORP
(72)Inventor : ASANO TOMOYUKI
OSAWA YOSHITOMO

(54) INFORMATION RECORDING APPARATUSINFORMATION REPRODUCING DEVICEINFORMATION RECORDING METHODINFORMATION REPRODUCING METHODAND INFORMATION RECORDING MEDIUMAND PROGRAM PROVIDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information recording apparatus and reproducing devices that can effectively exclude utilization of illegal contents.
SOLUTION: The recording medium of this invention stores secret information whose write/read method is difficult for its analysis and that can be read only by a special read methodand the secrete information is used for an encryption key for encryption or decoding processing of contents in recording or reproducing contents such as music data image data to/from the recording medium. The secret information is e.g. a stamper IDand the stamper ID as the secrete informationa master key and a medium key or the like distributed through key distribution configuration of a tree structure are used to generate an encryption processing key for contents. Thusa special read method as to the secret information can be performed and only a legal device to which the key is distributed through the key distribution configuration of a tree structure can utilize contents.

CLAIMS

[Claim(s)]
[Claim 1]The Information Storage Division device which records information on a recording mediumcomprising:

A cipher--processing means to perform encryption processing of stored data to a recording medium.
A confidential information decode processing means which reads confidential information which performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording medium.
Composition which performs cipher processing of data which it hasand said cipher-processing means generates a contents cryptographic key by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decode processing meansand is stored in a recording medium based on this contents cryptographic key.

[Claim 2]Said confidential information is stored in a recording medium at the time of manufacture of a recording mediumand in two or more recording media Common stamper IDOr disk ID peculiar to each recording mediumcontent ID differed and set up for every contentsOr the Information Storage Division device according to claim 1wherein said confidential information decode processing means has the composition which performs decoding processing of confidential information read in a recording medium including one data of the keys for cipher processing.
[Claim 3]Said cipher-processing means is adapted to use confidential information read in said confidential information decode processing meansand generate a contents cryptographic key.
The Information Storage Division device according to claim 1wherein read confidential information has available composition only in contents cryptographic key generation processing which does not perform a storing process to a memory measure in which reading from the Information Storage Division device outside is possiblebut is performed in said cipher-processing department.

[Claim 4]Said Information Storage Division device holds a node key peculiar to each node which constitutes a hierarchy tree structure which used several different Information Storage Division devices as a leaf furtherand a leaf key peculiar to each Information Storage Division deviceSaid cipher-processing means are confidential information read in said confidential information decode processing meansand composition which generates said contents cryptographic key based on data for cryptographic key generation built in said Information Storage Division device.
The Information Storage Division device according to claim 1wherein said data for cryptographic key generation is constituted as data which can be updated by validation key blocks (EKB) which enciphered a node key by a low order hierarchy's node key or a key of a leaf key which contains either at least.

[Claim 5]The Information Storage Division device according to claim 4wherein said data for cryptographic key generation is either of the medium keys peculiar to a common master key or a specific recording medium in two or more Information

Storage Division devices.
[Claim 6]Said data for cryptographic key generation is the composition that a generation number as update information was matched.
The Information Storage Division device according to claim 4wherein said cipher-processing part has the composition stored in said recording medium by making a generation number of said used data for cryptographic key generation into a record times cost number at the time of encryption data storage to said recording medium.

[Claim 7]Said Information Storage Division device has a transport stream processing means to add receiving time information (ATS) to each packet which constitutes further a transport stream which comprises a transport packetSaid cipher-processing means has the composition which generates a block key as a cryptographic key to block data which consists of one or more packets to which said receiving time information (ATS) was addedIn cipher processing of stored data to said recording mediumThe Information Storage Division device according to claim 4 having the composition which generates a block key as a cryptographic key based on data including said confidential informationand said data for cryptographic key generation and block seed who is additional information peculiar to block data including said receiving time information (ATS).
[Claim 8]It has the composition which performs decoding processing of data which said confidential information decode processing means carried out the turbulence of the bit string which forms confidential information according to a binary seriesand was stored in a recording mediumThe Information Storage Division device according to claim 1 having the composition which generates said binary seriesperforms data processing of a generation binary series and a regenerative signal from said recording mediumand performs decoding processing of confidential information.
[Claim 9]Data which said confidential information decode processing means was changed in accordance with a rule beforehand defined per two or more bits which constitutes confidential informationand was recorded is read in a recording mediumThe Information Storage Division device according to claim 1 having the composition which reconverts read data and performs decoding processing of confidential information.
[Claim 10]An information reproducing device which reproduces information recorded on a recording mediumcomprising:
A cipher--processing means to perform decoding processing of data read in a recording medium.
A confidential information decode processing means which reads confidential information which performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording medium.
Composition which performs decoding processing of data which it hasand said cipher-processing means generates a contents decryption key by using as data for

key generation confidential information which was read in a storage and decoded in said confidential information decode processing meansand is read in a recording medium based on this contents decryption key.

[Claim 11]Said confidential information is stored in a recording medium at the time of manufacture of a recording mediumand in two or more recording media Common stamper IDOr disk ID peculiar to each recording mediumcontent ID differed and set up for every contentsOr the information reproducing device according to claim 10wherein said confidential information decode processing means has the composition which performs decoding processing of confidential information read in a recording medium including one data of the keys for cipher processing.
[Claim 12]Confidential information read in said confidential information decode processing means is used for said cipher-processing meansAre adapted to generate a contents decryption key and read confidential information does not perform a storing process to a memory measure in which reading from the Information Storage Division device outside is possibleThe information reproducing device according to claim 10 having the composition made available only in contents decryption key generation processing performed in said cipher-processing department.
[Claim 13]The information reproducing device according to claim 10 constituting as data which can be updated by validation key blocks (EKB) characterized by comprising the following enciphered by a key.
Confidential information in which said information reproducing device held a node key peculiar to each node which constitutes a hierarchy tree structure which used several different information reproducing devices as a leaf furtherand a leaf key peculiar to each information reproducing deviceand said cipher-processing means was read in said confidential information decode processing means.
It is adapted to generate said contents decryption key based on data for decryption key generation built in said information reproducing deviceand a low order hierarchy's node key or a leaf key of said data for decryption key generation is either at least about a node key.

[Claim 14]The information reproducing device according to claim 13wherein said data for decryption key generation is either of the medium keys peculiar to a common master key or a specific recording medium in two or more information reproducing devices.
[Claim 15]Said data for decryption key generation is the composition that a generation number as update information was matched.
The information reproducing device according to claim 13wherein said cipher-processing part has the composition stored in said recording medium by making a generation number of said used data for decryption key generation into a record times cost number at the time of data reproduction from said recording medium.

[Claim 16]Said information reproducing device has a transport stream processing

means to add receiving time information (ATS) to each packet which constitutes further a transport stream which comprises a transport packetSaid cipher-processing means has the composition which generates a block key as a cryptographic key to block data which consists of one or more packets to which said receiving time information (ATS) was addedIn decoding processing of data from said recording mediumThe information reproducing device according to claim 13 having the composition which generates a block key as a decryption key based on data including said confidential informationand said data for decryption key generation and block seed who is additional information peculiar to block data including said receiving time information (ATS).

[Claim 17]It has the composition which performs decoding processing of data which said confidential information decode processing means carried out the turbulence of the bit string which forms confidential information according to a binary seriesand was stored in a recording mediumThe information reproducing device according to claim 10 having the composition which generates said binary seriesperforms data processing of a generation binary series and a regenerative signal from said recording mediumand performs decoding processing of confidential information.

[Claim 18]Data which said confidential information decode processing means was changed in accordance with a rule beforehand defined per two or more bits which constitutes confidential informationand was recorded is read in a recording mediumThe information reproducing device according to claim 10 having the composition which reconverts read data and performs decoding processing of confidential information.

[Claim 19]An Information Storage Division method which records information on a recording mediumcomprising:

A confidential information decoding processing step which reads confidential information which performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording medium.

A cipher-processing step which performs cipher processing of data which generates a contents cryptographic key by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decoding processing stepand is stored in a recording medium based on this contents cryptographic key.

[Claim 20]Said confidential information is stored in a recording medium at the time of manufacture of a recording mediumand in two or more recording media Common stamper IDOr disk ID peculiar to each recording mediumcontent ID differed and set up for every contentsOr an Information Storage Division method according to claim 19wherein said confidential information decoding processing step performs decoding processing of confidential information read in a recording medium including one data of the keys for cipher processing.

[Claim 21]Confidential information read in said confidential information decode

processing means is used for said cipher-processing stepRead confidential information does not perform a storing process to a memory measure in which reading from the Information Storage Division device outside is possible including a step which generates a contents cryptographic keyAn Information Storage Division method according to claim 19 supposing that it is available only in contents cryptographic key generation processing performed in said cipher-processing department.
[Claim 22]Said Information Storage Division method characterized by comprising the following.
Confidential information in which said cipher-processing step was read in said confidential information decode processing means.
Including a step which generates said contents cryptographic key based on data for cryptographic key generation built in the Information Storage Division devicesaid data for cryptographic key generationA low order hierarchy's node key or a leaf key is either at least about a node key of a hierarchy tree structure which used several different Information Storage Division devices as a leafand set up a key peculiar to each node and a leaf by making each branching into a node.

[Claim 23]An Information Storage Division method according to claim 22wherein said data for cryptographic key generation is either of the medium keys peculiar to a common master key or a specific recording medium in two or more Information Storage Division devices.
[Claim 24]Said data for cryptographic key generation is the composition that a generation number as update information was matched.
An Information Storage Division method according to claim 22wherein said cipher-processing step contains a step stored in said recording medium by making a generation number of said used data for cryptographic key generation into a record times cost number at the time of encryption data storage to said recording medium.

[Claim 25]Said Information Storage Division method has a transport stream processing step which adds receiving time information (ATS) to each packet which constitutes further a transport stream which comprises a transport packetSaid cipher-processing step contains a step which generates a block key as a cryptographic key to block data which consists of one or more packets to which said receiving time information (ATS) was addedIn cipher processing of stored data to said recording mediumAn Information Storage Division method according to claim 22 generating a block key as a cryptographic key based on data including said confidential informationand said data for cryptographic key generation and block seed who is additional information peculiar to block data including said receiving time information (ATS).
[Claim 26]Said confidential information decoding processing step contains a decoding processing step which performs decoding processing of data which carried out the turbulence of the bit string which forms confidential information

according to a binary seriesand was stored in a recording mediumAn Information Storage Division method according to claim 19 this decoding processing step's generating said binary seriesperforming data processing of a generation binary series and a regenerative signal from said recording mediumand performing decoding processing of confidential information.
[Claim 27]An Information Storage Division method according to claim 19 said confidential information decoding processing step's reading in a recording medium data changed and recorded in accordance with a rule beforehand defined per two or more bits which constitutes confidential informationreconverting read dataand performing decoding processing of confidential information.
[Claim 28]An information reproduction mode which reproduces information from a recording mediumcomprising:
A confidential information decoding processing step which reads confidential information which performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording medium.
A decoding processing step which performs decoding processing of data which generates a contents decryption key by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decoding processing stepand is read in a recording medium based on this contents decryption key.

[Claim 29]Said confidential information is stored in a recording medium at the time of manufacture of a recording mediumand in two or more recording media Common stamper IDOr disk ID peculiar to each recording mediumcontent ID differed and set up for every contentsOr the information reproduction mode according to claim 28wherein said confidential information decoding processing step performs decoding processing of confidential information read in a recording medium including one data of the keys for cipher processing.
[Claim 30]Confidential information read in said confidential information decode processing means is used for said decoding processing stepRead confidential information does not perform a storing process to a memory measure in which reading from the Information Storage Division device outside is possible including a step which generates a contents decryption keyThe information reproduction mode according to claim 28 supposing that it is available only in contents decryption key generation processing performed in said cipher-processing department.
[Claim 31]In said information reproduction modesaid decoding processing stepConfidential information read in said confidential information decode processing means and a step which generates said contents decryption key based on data for decryption key generation built in an information reproducing device are includedSaid data for decryption key generation uses several different information reproducing devices as a leafMake each branching into a node and Each nodeThe information reproduction mode according to claim 28 being data

which can be updated by validation key blocks (EKB) which enciphered a node key of a hierarchy tree structure which set up a key peculiar to a leaf by a low order hierarchy's node key or a key of a leaf key which contains either at least.
[Claim 32]The information reproduction mode according to claim 31wherein said data for decryption key generation is either of the medium keys peculiar to a common master key or a specific recording medium in two or more information reproducing devices.
[Claim 33]Said data for decryption key generation is the composition that a generation number as update information was matched.
The information reproduction mode according to claim 31wherein said decoding processing step contains a step stored in said recording medium by making a generation number of said used data for decryption key generation into a record times cost number at the time of data reproduction from said recording medium.

[Claim 34]Said information reproduction mode has a transport stream processing step which adds receiving time information (ATS) to each packet which constitutes further a transport stream which comprises a transport packetSaid decoding processing step contains a step which generates a block key as a cryptographic key to block data which consists of one or more packets to which said receiving time information (ATS) was addedIn regeneration of data from said recording mediumThe information reproduction mode according to claim 31 generating a block key as a decryption key based on data including said confidential informationand said data for decryption key generation and block seed who is additional information peculiar to block data including said receiving time information (ATS).
[Claim 35]Said confidential information decoding processing step contains a decoding processing step which performs decoding processing of data which carried out the turbulence of the bit string which forms confidential information accordirg to a binary seriesand was stored in a recording mediumThe information reproduction mode according to claim 28 this decoding processing step's generating said binary seriesperforming data processing of a generation binary series and a regenerative signal from said recording mediumand performing decoding processing of confidential information.
[Claim 36]The information reproduction mode according to claim 28 said confidential information decoding processing step's reading in a recording medium data changed and recorded in accordance with a rule beforehand defined per two or more bits which constitutes confidential informationreconverting read dataand performing decoding processing of confidential information.
[Claim 37]By performing special data reading processing which is an information recording medium which can record information and is usually different from a reading mode of stored dataaccept it and Refreshable confidential informationAn information recording medium storing enciphered content which can be decoded with a generable cipher-processing key with the application of this confidential information.

[Claim 38]The information recording medium according to claim 37wherein said confidential information contains data of either common stamper ID or disk ID peculiar to each recording mediumcontent ID differed and set up for every contents or a key for cipher processing in two or more recording media.
[Claim 39]It is a program providing medium which provides a computer program which makes the Information Storage Division processing which records information on a recording medium perform on computer systemsA confidential information decoding processing step which reads confidential information which said computer program performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording mediumA contents cryptographic key is generated by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decoding processing stepA program providing medium having a cipher-processing step which performs cipher processing of data stored in a recording medium based on this contents cryptographic key.
[Claim 40]It is a program providing medium which provides a computer program which makes information reproduction processing which reproduces information stored in a recording medium perform on computer systemsA confidential information decoding processing step which reads confidential information which said computer program performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording mediumA contents decryption key is generated by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decoding processing stepA program providing medium having a decoding processing step which performs decoding processing of data read in a recording medium based on this contents decryption key.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]In this inventionthe hierarchical key distribution system of a tree structure is especially used about the Information Storage Division devicean information reproducing devicethe Information Storage Division methodan information reproduction modean information recording mediumand a program providing medium.
Therefore,while providing the composition which made it possible to press down the amount of messages small and to reduce the load of the data distribution in the renewal of a key of a master key or a medium keyBy composition which applies the confidential information which can be read only in different special data reading processing from regeneration of contents as generated data of the key for cipher processing of contents. It is related with the Information Storage Division devicethe information reproducing devicethe Information Storage Division

methodinformation reproduction mode and information recording medium which made it possible to raise the security of contentsand a program providing medium.

[0002]Via a recording medium or a communication line specifically using the key distribution method of composition of having arranged each record reproducer apparatus to each wooden leaf (leaf) for n minutesWhile a key (a master key or a medium key) required for the record to the recording medium of contents data or the reproduction from a recording medium is distributed and each device performs record of contents dataand reproduction using thisStamper ID etc. are stored in contents recording and the contents storing disk for playback as confidential informationIt is related with the Information Storage Division devicethe information reproducing devicethe Information Storage Division methodinformation reproduction mode and information recording medium which were considered as the composition which acquires confidential information and generates the key for cipher processing of contents based on acquisition confidential information by specific regenerationand a program providing medium.
[0003]
[Description of the Prior Art]In recent yearsthe recorder and recording medium which record information in digital one are spreading with progress of digital-signal-processing art and development. According to such a digital recording device and a recording mediumrecord and reproduction can be repeatedwithout degrading a picture and a soundfor example. Thussince the digital data can carry out repeat execution of the copy repeatedlywith image quality or tone quality maintainedWhen the recording medium with which the copy was performed illegally will circulate in a commercial sceneprofitssuch as an owner of a copyright of various contentssuch as music and a movieor a just dealership personwill be injured. In these daysin order to prevent the unjust copy of such digital datavarious structure (system) for preventing an illegal copy is introduced into the digital recording device and the recording medium.
[0004]For examplein MD (mini disc) (MD is trademark) deviceSCMS (Serial Copy Management System) is adopted as a method of preventing an illegal copy. In [SCMS outputs a SCMS signal to the data reproduction side from a digital interface (DIF) with audio informationand] the Data Recording Sub-Division sideIt is a system which prevents an illegal copy by controlling record of the audio information from the reproduction side based on the SCMS signal from the reproduction side.
[0005]A SCMS signal specifically. [whether audio information is data of copy free (copy free) in which a copy is permitted any number of timesand] It is a signal showing whether it is data in which the copy is allowed only once (copy once allowed)or it is data in which the copy is forbidden (copy prohibited). If audio information is received from DIF to the Data Recording Sub-Division sidethe SCMS signal transmitted with the audio information will be detected. And when the SCMS signal serves as copy free (copy free)audio information is recorded on a mini disc with a SCMS signal. When the SCMS signal is permitted (copy once

allowed) once about the copya SCMS signal is changed into copy prohibition (copy prohibited)and it records on a mini disc with audio information. Audio information is not recorded when the SCMS signal serves as copy prohibition (copy prohibited). By performing control which uses such SCMSthe audio information which has copyright prevents being copied illegally by SCMS with a mini disc device.
[0006]Howeversince it is a premise that the apparatus itself which records data has the composition which controls record of the audio information from the reproduction side based on a SCMS signal as mentioned above as for SCMSWhen a mini disc device without the composition which performs control of SCMS is manufacturedit becomes difficult to cope with it. Thenfor examplewith the DVD playerit has the composition of preventing the illegal copy of data which has copyrightby adopting a contents scramble system.
[0007]In a contents scramble systemto DVD-ROM (Read Only Memory). A video dataaudio informationetc. are enciphered and recorded and the key (decode key) used for decoding the enciphered data is given to the licensed DVD player. It is licensed to the DVD player designed follow predetermined regulation of not copying illegally of operation. Thereforein the licensed DVD playeran image and a sound are renewable from DVD-ROM by decoding the encryption data recorded on DVD-ROM using the given key.
[0008]On the other handsince the DVD player which has not been licensed does not have a key for decoding the enciphered datait cannot decode the encryption data recorded on DVD-ROM. Thusin contents scramble system compositionthe DVD player which does not fulfill the conditions demanded at the time of a license can reproduce DVD-ROM which recorded the digital dataand an illegal copy is prevented.
[0009]Howeverthe contents scramble system adopted with DVD-ROM is aimed at the recording medium (suitably henceforth ROM media) which cannot write in the data by a user.
It is not taken into consideration about application to the recording medium (suitably henceforth RAM media) which can write in the data by a user.

[0010]That iseven if the data recorded on ROM media was encipheredwhen the enciphered data is all copied to RAM media as it waswhat is called a refreshable pirate edition will be able to be created with the licensed just device.
[0011]Thenin previous patent application and JPH11-224461A (Tokuganhei10-25310) these peopleRecord the information (it is hereafter described as medium identification information) for identifying each recording medium on a recording medium with other dataand on condition that it is the device which received the license of this medium identification informationit carries outOnly when the condition was fulfilledthe composition whose access to the medium identification information of a recording medium is attained was proposed.
[0012]The data on a recording medium is enciphered in this method by the secret key (master key) obtained by receiving medium identification information and a licenseMeaningful data cannot be obtained even if the device which has not been

licensed reads this enciphered data. When a device is licensedthe operation is specified so that an unjust duplicate (illegal copy) may not be made.
[0013]Since the device which has not been licensed cannot access medium identification information and medium identification information serves as an individual value for each medium of everyEven if the device which has not been licensed reproduces all the enciphered data that is recorded on the recording medium to a new recording mediumSince the data recorded on the recording medium created by making it such cannot be correctly decoded in the licensed device as well as the device which has not been licensedan illegal copy will be prevented substantially.
[0014]
[Problem(s) to be Solved by the Invention]By the wayas for the master key stored in the licensed devicein the above-mentioned compositionit is common in a complete aircraft machine that it is common. Thusit is because it is conditions required in order that storing a common master key to two or more apparatus may make refreshable the medium recorded by one apparatus by other apparatus (interoperability is secured).
[0015]Howeverin this methodwhen an aggressor succeeds in the attack of one apparatus and takes out a master keythe data currently enciphered and recorded in all the systems can be decodedand the whole system collapses. In order to prevent thiswhen what a certain apparatus was attacked and the master key exposed is revealedit is necessary to give the master key which updated the master key to a new thing and was newly updated by complete aircraft machines other than the apparatus which yielded to the attack. Although the peculiar key (debye skiing) is given to each apparatus as a method simple No. 1 which realizes this compositionthe value which enciphered a new master key on each debye skis is prepared and the method transmitted to apparatus via a recording medium can be consideredThere is a problem that the total amount of messages which should be transmitted in proportion to the number of apparatus increases.
[0016]As composition which solves the above-mentioned problemthese peopleVia a recording medium or a communication line using the key distribution method of composition of having arranged each Information Storage Division playback equipment to each wooden leaf (leaf) for n minutesWhen a key (a master key or a medium key) required for the record to the recording medium of contents data or the reproduction from a recording medium is distributed and each device is made to perform record of contents dataand reproduction using thisThe just (to device which the secret has not exposed) composition which receives and can transmit a master key or a medium key in the small amount of messages is proposed previouslyand patent application has already been carried out. The key which is specifically needed in order to generate a key required for the record to a recording mediumor the reproduction from a recording mediumFor examplethe node key assigned to the node which constitutes each wooden leaf (leaf) for n minutes is set up as an updating node keyThe leaf key in which only just apparatus has an updating node keyand validation key blocks (EKB) including the information

which carried out encryption processing in the mode which can decode by a node key are distributed to each Information Storage Division playback equipmentIt is the composition which made acquirable the key which each device needs for record or the reproduction from a recording medium by the EKB decoding processing of each Information Storage Division playback equipment which received validation key blocks (EKB).
[0017]The antecedent basis of the safety is placed by that neither the encryption key given to Information Storage Division playback equipment nor the medium key used for the encryption/decoding processing at the time of record/reproduction of the data to a recording medium exposes above-mentioned composition.
Thereforeit will be satisfactory if disclosure of a medium key can be prevented.
Howeverif exposed of the medium key which should be made secretit has quite a few influences on the system.
[0018]The purpose of this invention is as follows.
In [aim at solving the above-mentioned problem and] the usual data reading techniqueEnable exclusion of the illegal use of contents by considering confidential information which the analysis of data wrote in with difficult composition as the composition used as data for key generation used for the encryption/decoding processing at the time of record/reproduction of the data to a recording medium.
Provide the high Information Storage Division device of the security which made the possibility of disclosure of the seed data for keys used for the encryption/decoding processing at the time of record/reproduction decrease sharplyan information reproducing devicethe Information Storage Division methodan information reproduction modean information recording mediumand a program providing medium.

[0019]
[Means for Solving the Problem]In the Information Storage Division device with which the 1st side of this invention records information on a recording mediumA cipher-processing means to perform encryption processing of stored data to a recording mediumA confidential information decode processing means which reads confidential information which performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording medium**** and said cipher-processing means generates a contents cryptographic key by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decode processing meansIt is in the Information Storage Division device having the composition which performs cipher processing of data stored in a recording medium based on this contents cryptographic key.
[0020]The Information Storage Division device of this invention sets like 1 operative conditionand said confidential informationIt is stored in a recording medium at the time of manufacture of a recording mediumand in two or more recording media Common stamper IDOr said confidential information decode processing means has the composition which performs decoding processing of

confidential information read in a recording medium including data of either disk ID peculiar to each recording mediumcontent ID differed and set up for every contents or a key for cipher processing.
[0021]The Information Storage Division device of this invention sets like 1 operative conditionand said cipher-processing meansConfidential information read in said confidential information decode processing means is usedIt is adapted to generate a contents cryptographic keyand read confidential information did not perform a storing process to a memory measure in which reading from the Information Storage Division device outside is possiblebut it had available composition only in contents cryptographic key generation processing performed in said cipher-processing department.
[0022]The Information Storage Division device of this invention sets like 1 operative conditionand said Information Storage Division deviceHold a node key peculiar to each node which constitutes a hierarchy tree structure which used several different Information Storage Division devices as a leafand a leaf key peculiar to each Information Storage Division deviceand said cipher-processing meansThey are confidential information read in said confidential information decode processing meansand the composition which generates said contents cryptographic key based on data for cryptographic key generation built in said Information Storage Division deviceSaid data for cryptographic key generation is constituted as data which can be updated by validation key blocks (EKB) which enciphered a node key by a low order hierarchy's node key or a key of a leaf key which contains either at least.
[0023]The Information Storage Division device of this invention sets like 1 operative conditionand said data for cryptographic key generation is characterized by being either of the medium keys peculiar to a common master key or a specific recording medium in two or more Information Storage Division devices.
[0024]The Information Storage Division device of this invention sets like 1 operative conditionand said data for cryptographic key generationIt is the composition that a generation number as update information was matchedand said cipher-processing part has the composition stored in said recording medium by making a generation number of said used data for cryptographic key generation into a record times cost number at the time of encryption data storage to said recording medium.
[0025]The Information Storage Division device of this invention sets like 1 operative conditionand it has a transport stream processing means to add receiving time information (ATS) to each packet which constitutes a transport stream which comprises a transport packetSaid cipher-processing means has the composition which generates a block key as a cryptographic key to block data which consists of one or more packets to which said receiving time information (ATS) was addedIn cipher processing of stored data to said recording mediumIt has the composition which generates a block key as a cryptographic key based on data including said confidential informationand said data for cryptographic key generation and block seed who is additional information peculiar to block data

including said receiving time information (ATS).
[0026]The Information Storage Division device of this invention sets like 1 operative conditionand said confidential information decode processing meansIt has the composition which performs decoding processing of data which carried out the turbulence of the bit string which forms confidential information according to a binary seriesand was stored in a recording mediumIt has the composition which generates said binary seriesperforms data processing of a generation binary series and a regenerative signal from said recording mediumand performs decoding processing of confidential information.
[0027]The Information Storage Division device of this invention sets like 1 operative conditionand said confidential information decode processing meansIt has the composition which reads in a recording medium data changed and recorded in accordance with a rule beforehand defined per two or more bits which constitutes confidential informationreconverts read dataand performs decoding processing of confidential information.
[0028]In an information reproducing device with which the 2nd side of this invention reproduces information recorded on a recording mediumA cipher-processing means to perform decoding processing of data read in a recording mediumA confidential information decode processing means which reads confidential information which performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording medium**** and said cipher-processing means generates a contents decryption key by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decode processing meansIt is in an information reproducing device having the composition which performs decoding processing of data read in a recording medium based on this contents decryption key.
[0029]An information reproducing device of this invention sets like 1 operative conditionand said confidential informationIt is stored in a recording medium at the time of manufacture of a recording mediumand in two or more recording media Common stamper IDOr said confidential information decode processing means has the composition which performs decoding processing of confidential information read in a recording medium including data of either disk ID peculiar to each recording mediumcontent ID differed and set up for every contents or a key for cipher processing.
[0030]An information reproducing device of this invention sets like 1 operative conditionand said cipher-processing meansConfidential information read in said confidential information decode processing means is usedIt is adapted to generate a conterts decryption keyand read confidential information does not perform a storing process to a memory measure in which reading from the Information Storage Division device outside is possiblebut it has the composition made available only in contents decryption key generation processing performed in said cipher-processing department.
[0031]A leaf key peculiar to a node key peculiar to each node which constitutes a

hierarchy tree structure which set like 1 operative condition and used several different information reproducing devices as a leaf and each information reproducing device of an information reproducing device of this invention is heldConfidential information in which said cipher-processing means was read in said confidential information decode processing meansAre adapted to generate said contents decryption key based on data for decryption key generation built in said information reproducing deviceand said data for decryption key generationIt is constituted as data which can be updated by validation key blocks (EKB) which enciphered a node key by a low order hierarchy's node key or a key of a leaf key which contains either at least.

[0032]An information reproducing device of this invention sets like 1 operative conditionand said data for decryption key generation is characterized by being either of the medium keys peculiar to a common master key or a specific recording medium in two or more information reproducing devices.

[0033]An information reproducing device of this invention sets like 1 operative conditionand said data for decryption key generationIt is the composition that a generation number as update information was matchedand said cipher-processing part has the composition stored in said recording medium by making a generation number of said used data for decryption key generation into a record times cost number at the time of data reproduction from said recording medium.

[0034]An information reproducing device of this invention sets like 1 operative conditionand it has a transport stream processing means to add receiving time information (ATS) to each packet which constitutes a transport stream which comprises a transport packetSaid cipher-processing means has the composition which generates a block key as a cryptographic key to block data which consists of one or more packets to which said receiving time information (ATS) was addedIn decoding processing of data from said recording mediumIt has the composition which generates a block key as a decryption key based on data including said confidential informationand said data for decryption key generation and block seed who is additional information peculiar to block data including said receiving time information (ATS).

[0035]An information reproducing device of this invention sets like 1 operative conditionand said confidential information decode processing meansIt has the composition which performs decoding processing of data which carried out the turbulence of the bit string which forms confidential information according to a binary seriesand was stored in a recording mediumIt has the composition which generates said binary seriesperforms data processing of a generation binary series and a regenerative signal from said recording mediumand performs decoding processing of confidential information.

[0036]An information reproducing device of this invention sets like 1 operative conditionand said confidential information decode processing meansIt has the composition which reads in a recording medium data changed and recorded in accordance with a rule beforehand defined per two or more bits which constitutes confidential informationreconverts read dataand performs decoding processing of

confidential information.
[0037]In an Information Storage Division method that the 3rd side of this invention records information on a recording mediumA confidential information decoding processing step which reads confidential information which performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording mediumA contents cryptographic key is generated by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decoding processing stepIt is in an Information Storage Division method having a cipher-processing step which performs cipher processing of data stored in a recording medium based on this contents cryptographic key.
[0038]An Information Storage Division method of this invention sets like 1 operative conditionand said confidential informationIt is stored in a recording medium at the time of manufacture of a recording mediumand in two or more recording media Common stamper IDOr said confidential information decoding processing step performs decoding processing of confidential information read in a recording medium including data of either disk ID peculiar to each recording mediumcontent ID differed and set up for every contents or a key for cipher processing.
[0039]An Information Storage Division method of this invention sets like 1 operative conditionand said cipher-processing stepConfidential information read in said confidential information decode processing means is usedConfidential information read including a step which generates a contents cryptographic key did not perform a storing process to a memory measure in which reading from the Information Storage Division device outside is possiblebut presupposed that it is available only in contents cryptographic key generation processing performed in said cipher-processing department.
[0040]An Information Storage Division method of this invention sets like 1 operative conditionand said cipher-processing stepConfidential information read in said confidential information decode processing means and a step which generates said contents cryptographic key based on data for cryptographic key generation built in the Information Storage Division device are includedSaid data for cryptographic key generation uses several different Information Storage Division devices as a leafIt is characterized by being data which can be updated by validation key blocks (EKB) which enciphered a node key of a hierarchy tree structure which set up a key peculiar to each node and a leaf by making each branching into a node by a low order hierarchy's node key or a key of a leaf key which contains either at least.
[0041]An Information Storage Division method of this invention sets like 1 operative conditionand said data for cryptographic key generation is characterized by being either of the medium keys peculiar to a common master key or a specific recording medium in two or more Information Storage Division devices.
[0042]An Information Storage Division method of this invention sets like 1 operative conditionand said data for cryptographic key generationIt is the

composition that a generation number as update information was matchedand said cipher-processing step contains a step stored in said recording medium by making a generation number of said used data for cryptographic key generation into a record times cost number at the time of encryption data storage to said recording medium.

[0043]An Information Storage Division method of this invention sets like 1 operative conditionand said Information Storage Division methodIt has a transport stream processing step which adds receiving time information (ATS) to each packet which constitutes a transport stream which comprises a transport packetSaid cipher-processing step contains a step which generates a block key as a cryptographic key to block data which consists of one or more packets to which said receiving time information (ATS) was addedIn cipher processing of stored data to said recording mediumA block key as a cryptographic key is generated based on data including said confidential informationand said data for cryptographic key generation and block seed who is additional information peculiar to block data including said receiving time information (ATS).

[0044]An Information Storage Division method of this invention sets like 1 operative conditionand said confidential information decoding processing stepDecoding processing of data which carried out the turbulence of the bit string which forms confidential information according to a binary seriesand was stored in a recording medium including a decoding processing step to perform this decoding processing stepSaid binary series is generateddata processing of a generation binary series and a regenerative signal from said recording medium is performedand decoding processing of confidential information is performed.

[0045]An Information Storage Division method of this invention sets like 1 operative conditionand said confidential information decoding processing stepData changed and recorded in accordance with a rule beforehand defined per two or more bits which constitutes confidential information is read in a recording mediumread data is reconvertedand decoding processing of confidential information is performed.

[0046]In an information reproduction mode with which the 4th side of this invention reproduces information from a recording mediumA confidential information decoding processing step which reads confidential information which performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording mediumA contents decryption key is generated by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decoding processing stepIt is in an information reproduction mode having a decoding processing step which performs decoding processing of data read in a recording medium based on this contents decryption key.

[0047]An information reproduction mode of this invention sets like 1 operative conditionand said confidential informationIt is stored in a recording medium at the time of manufacture of a recording mediumand in two or more recording media

Common stamper IDOr said confidential information decoding processing step performs decoding processing of confidential information read in a recording medium including data of either disk ID peculiar to each recording mediumcontent ID differed and set up for every contents or a key for cipher processing.
[0048]An information reproduction mode of this invention sets like 1 operative conditionand said decoding processing stepConfidential information read in said confidential information decode processing means is usedConfidential information read including a step which generates a contents decryption key did not perform a storing process to a memory measure in which reading from the Information Storage Division device outside is possiblebut presupposed that it is available only in contents decryption key generation processing performed in said cipher-processing department.
[0049]An information reproduction mode of this invention sets like 1 operative conditionand said decoding processing stepConfidential information read in said confidential information decode processing means and a step which generates said contents decryption key based on data for decryption key generation built in an information reproducing device are includedSaid data for decryption key generation uses several different information reproducing devices as a leafIt is characterized by being data which can be updated by validation key blocks (EKB) which enciphered a node key of a hierarchy tree structure which set up a key peculiar to each node and a leaf by making each branching into a node by a low order hierarchy's node key or a key of a leaf key which contains either at least.
[0050]An information reproduction mode of this invention sets like 1 operative conditionand said data for decryption key generation is characterized by being either of the medium keys peculiar to a common master key or a specific recording medium in two or more information reproducing devices.
[0051]An information reproduction mode of this invention sets like 1 operative conditionand said data for decryption key generationIt is the composition that a generation number as update information was matchedand said decoding processing step contains a step stored in said recording medium by making a generation number of said used data for decryption key generation into a record times cost number at the time of data reproduction from said recording medium.
[0052]An information reproduction mode of this invention sets like 1 operative conditionhave a transport stream processing step which adds receiving time information (ATS) to each packet which constitutes a transport stream which comprises a transport packetand said decoding processing stepIn regeneration of data from said recording mediumincluding a step which generates a block key as a cryptographic key to block data which consists of one or more packets to which said receiving time information (ATS) was addedsaid confidential informationA block key as a decryption key is generated based on data including said data for decryption key generationand block seed who is additional information peculiar to block data including said receiving time information (ATS).
[0053]An information reproduction mode of this invention sets like 1 operative conditionand said confidential information decoding processing stepDecoding

processing of data which carried out the turbulence of the bit string which forms confidential information according to a binary seriesand was stored in a recording medium including a decoding processing step to perform this decoding processing stepSaid binary series is generateddata processing of a generation binary series and a regenerative signal from said recording medium is performedand decoding processing of confidential information is performed.
[0054]An information reproduction mode of this invention sets like 1 operative conditionand said confidential information decoding processing stepData changed and recorded in accordance with a rule beforehand defined per two or more bits which constitutes confidential information is read in a recording mediumread data is reconvertedand decoding processing of confidential information is performed.
[0055]By performing special data reading processing which the 5th side of this invention is an information recording medium which can record informationand is usually different from a reading mode of stored dataaccept it and Refreshable confidential informationIt is in an information recording medium storing enciphered content which can be decoded with a generable cipher-processing key with the application of this confidential information.
[0056]An information recording medium of this invention sets like 1 operative conditionand said confidential informationIn two or more recording mediadata of either common stamper ID or disk ID peculiar to each recording mediumcontent ID differed and set up for every contents or a key for cipher processing is included.
[0057]The 6th side of this invention is a program providing medium which provides a computer program which makes the Information Storage Division processing which records information on a recording medium perform on computer systemsA confidential information decoding processing step which reads confidential information which said computer program performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording mediumA contents cryptographic key is generated by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decoding processing stepIt is in a program providing medium having a cipher-processing step which performs cipher processing of data stored in a recording medium based on this contents cryptographic key.
[0058]The 7th side of this invention is a program providing medium which provides a computer program which makes information reproduction processing which reproduces information stored in a recording medium perform on computer systemsA confidential information decoding processing step which reads confidential information which said computer program performed different special data reading processing from a reading mode of contents data stored in a recording mediumand was stored in a recording mediumA contents decryption key is generated by using as data for key generation confidential information which was read in a storage and decoded in said confidential information decoding processing stepIt is in a program providing medium having a decoding processing step which performs decoding processing of data read in a recording medium

based on this contents decryption key.
[0059]
[Function]In the composition of this inventionthe signal which becomes a recording medium from the difficult confidential information of the analysis of its writing / the read-out method beforehand is embedded. The above-mentioned confidential information is made to act on the encryption key for performing the data encryption/decoding processing at the time of performing record/reproduction of data to this recording medium. How to read confidential information and the read secret value are composition which it is mounted for examplein LSIis highly protectedand is not exposed within a recording and reproducing device. Since it is such compositioneven if exposed of other encryption keysthe data stored as confidential information on the recording medium can be protected safely. Since the encryption key for performing various contents data encryption / decoding processingssuch as music on a recording mediumwill be generated using confidential informationprocessing of unjust decoding of the contents themselvesetc. becomes difficultand the contents protection with a high security level is attained.
[0060]The program providing medium concerning the 6th and 7th sides of this inventior is a medium which provides a computer program in a computer-readable form to the general purpose computer system which can execute various program codesfor example. As for a mediumthe gestalten in particularsuch as transmission mediasuch as recording mediasuch as CDFDMOor a networkare not limited.
[0061]Such a program providing medium defines the collaboration relation on the structure of the computer program and distribution medium for realizing the function of a predetermined computer programor a function on computer systems. If it puts in another wayby installing a computer program in computer systems via this distribution mediumon computer systemsa collaboration operation is demonstrated and the same operation effect as other sides of this invention can be obtained.
[0062]The purposethe featureand advantage of further others of this invention will become clear [rather than] by detailed explanation based on working example and the Drawings to attach of this invention mentioned later.
[0063]
[Embodiment of the Invention][System configuration] Drawing 1 is a block diagram showing one working example composition of the recording and reproducing device 100 which applied this invention. The recording and reproducing device 100Input-and-output I/F. 120 (Interface) MPEG (Moving.) Input-and-output I/F(Interface) 140 [provided with the Picture Experts Group codec 130A/Dand D/A converter 141]the cipher-processing means 150ROM(Read Only Memory) 160CPU (Central.) It has the drive 190 of Processing Unit170the memory 180and the recording medium 195 and also the transport stream processing means (TS processing means) 300and the confidential information decode processing means 500and these are mutually connected by bus 110.
[0064]Input-and-output I/F120 receives the digital signal on the bus 110and

outputs it outside while it receives the digital signal which constitutes various contents supplied from the outsidesuch as a picturea soundand a programand outputs it on the bus 110. The MPEG codec 130 carries out MPEG encoding of the digital signal supplied from input-and-output I/F140and outputs it on the bus 110 while it carries out MPEG decoding of the data which is supplied via the bus 110 and by which MPEG coding was carried out and outputs it to input-and-output I/F140. Input-and-output I/F140 builds in A/D and D/A converter 141. It is input-and-output I/F140 receiving the analog signal as contents supplied from the outsideand carrying out A/D (Analog Digital) conversion by A/D and D/A converter 141As a digital signalwhile outputting to the MPEG codec 130the digital signal from the MPEG codec 130 is outputted outside as an analog signal by carrying out D/A (Digital Analog) conversion by A/D and D/A converter 141.
[0065]For example the cipher-processing means 150 comprises LSI (Large Scale IntegratedCircuit) of one chipenciphers or decodes the digital signal as contents supplied via the bus 110and has the composition outputted on the bus 110. Not only 1 chip LSI but the thing which the composition which combined various kinds of software or hardwares realizes is possible for the cipher-processing means 150. The latter part explains the composition as a processing means by a software configuration.
[0066]ROM160 has memorized the leaf key which is peculiar debye skiingand the node key which are two or more recording and reproducing devices or debye skiing shared in two or more groups for every recording and reproducing device for every group of two or more peculiar or recording and reproducing devicesfor example. CPU170 is executing the program memorized by the memory 180and controls the MPEG codec 130 and cipher-processing means 150 grade. The memory 180 is nonvolatile memory and memorizes required data on the program which CPU170 executesand operation of CPU170for example. While the drive 190 reads digital data from the recording medium 195 (reproducing) and outputs it on the bus 110 by driving the recording medium 195 in which record reproduction is possible for digital dataThe digital data supplied via the bus 110 is supplied to the recording medium 195and is made to record. A program may be memorized to ROM160 and it may be made to memorize debye skiing in the memory 180.
[0067]The recording medium 195 is a medium which can memorize digital datasuch as semiconductor memorysuch as optical discssuch as DVD and CDa magneto-optical disca magnetic diskmagnetic tapeor RAMfor example.
According to this embodimentsuppose that it is removable composition to the drive 190.
Howeverthe recording medium 195 is good also as composition built in the recording and reproducing device 100.
[0068]Although the transport stream processing means (TS processing means) 300 is explained in detail below using drawing 6 in the latter partFor examplethe transport packet corresponding to a specific program (contents) is taken out from the transport stream which two or more TV programs (contents) multiplexedData processing for storing the appearance timing information of the taken-out

transport stream in the recording medium 195 with each packet and appearance timing-control processing at the time of the regeneration from the recording medium 195 are performed.
[0069]ATS (Arrival Time Stamp: mail arrival time stamp) as appearance timing information of each transport packet is set to the transport stream.
It is determined at the time of coding that this timing will not ruin T-STD (Transport stream System Target Decoder) which is the virtual decoder specified with MPEG 2 systemsand at the time of reproduction of a transport stream.
Appearance timing is controlled by ATS added to each transport packet.
The transport stream processing means (TS processing means) 300 performs these control. For examplein recording a transport packet on a recording mediumrecord as a source packet which packed the interval of each packetbut. By saving the appearance timing of each transport packet collectively at a recording mediumit becomes possible to control the output timing of each packet at the time of reproduction. The transport stream processing means (TS processing means) 300 adds and records ATS (ArrivalTime Stamp: mail arrival time stamp) showing the input timing of each transport packet at the time of Data Recording Sub-Division to the recording media 195such as DVD.
[0070]In the cipher-processing means 150the recording and reproducing device 100 of this invention performs encryption processing about the contents constituted by the transport stream to which above-mentioned ATS was addedand stores in the recording medium 195 the contents by which encryption processing was made. The cipher-processing means 150 performs decoding processing of the enciphered content stored in the recording medium 195. The latter part explains the details of these processings.
[0071]The confidential information decode processing means 500 is a processing means to perform reproduction of the confidential information which can be readand decoding processing by special regeneration stored in the recording medium 195. Stamper ID to which the confidential information stored in the recording medium 195 is setfor example for every stamper of ****** of a diskThey are various identification datasuch as disk ID set up by differing for every diskcontent ID differed and set up for every contentsor a key for cipher processinga cipher-processing keyetc.
[0072]The confidential information decode processing means 500 reads the confidential information stored in the recording medium 195decodesand transmits the decoded confidential information to the cipher-processing means 150. The cipher-processing means 150 generates the contents recording over a recording mediumand the cipher-processing key applied at the time of reproduction using confidential information. The confidential information decoded in the confidential information decode processing means 500 does not perform the storing process to the memory measure in which reading from the recording and reproducing device outside s possibleIt is the composition used only in the contents cryptographic key generation performed within the cipher-processing means 150and has the composition of having prevented the disclosure to the exterior of confidential

information.
[0073]The cipher-processing means 150TS processing means 300and the confidential information decode processing means 500 which are shown in drawing 1 are shown as another block in order to understand easilybut. It is good also as composition which may constitute as one or more LSI which performs each functionand realizes either of each function by composition which combined software or hardware.
[0074]The composition shown in drawing 2 other than composition of being shown in drawing 1 as an example of composition of the recording and reproducing device of this invention is possible. The recording medium 205 can be detached and attached from the recording-medium interface (I/F) 210 as a drive deviceand in the recording and reproducing device 200 shown in drawing 2even if it equips another recording and reproducing device with this recording medium 205it is considered as the composition in which read-out of data and writing are possible.
[0075][The Data Recording Sub-Division processing and data reproduction processing] Nextthe Data Recording Sub-Division processing and the data reproduction processing from a recording medium to drawing 1 or the recording medium in the recording and reproducing device of drawing 2 are explained with reference to the flow chart of drawing 3 and drawing 4. When recording the contents of the digital signal from the outside on the recording medium 195recording processing according to the flow chart of drawing 3 (A) is performed. Namelythe contents (digital contents) of a digital signal. For examplevia IEEE(Institute of Electrical and Electronics Engineers) 1394 serial bus etc.If input-and-output I/F120 is suppliedin Step S301input-and-output I/F120 will receive the digital contents suppliedand will output them to TS processing means 300 via the bus 110.
[0076]In Step S302TS processing means 300 generates the block data which added ATS to each transport packet which constitutes a transport streamand outputs it to the cipher-processing means 150 via the bus 110.
[0077]In Step S303the cipher-processing means 150 performs encryption processing to the digital contents which receivedand outputs the enciphered content obtained as a result to the drive 190 or recording-medium I/F210 via the bus 110. Enciphered content is recorded on the recording medium 195 via the drive 190 or recording-medium I/F210 (S304)and ends recording processing. The latter part explains cipher processing in the cipher-processing means 150.
[0078]Between [connected via the IEEE1394 serial bus] devicesBy five companies which include Sony Corp. which is this Applicant as a standard for protecting digital contents when transmitting digital contents. Although 5CDTCP (Five Company Digital Transmission Content Protection) (suitably henceforth DTCP) is definedWhen the digital contents which are not free as for a copy are transmitted between devices in this DTCPIn [attest mutually whether in advance of data communicationsthe transmitting side and a receiver can deal with the copy control information for controlling a copy correctlyand] after that and the transmitting sideDigital contents are enciphered and transmitted and the

enciphered digital contents (enciphered content) are decoded in a receiver.
[0079]In the data transmission and reception based on a standard to this DTCPInput-and-output I/F120 of a data receiving side is Step S301it receives enciphered content via an IEEE1394 serial busdecodes the enciphered content to DTCP based on a standardand outputs it to the cipher-processing means 150 after that as contents of a plaintext.
[0080]The key which carries out a temporal change is generated and encryption of the digital contents by DTCP is performed using the key. The enciphered digital contents are transmitted in IEEE1394 serial bus tops including the key used for the encryptionand decode the enciphered digital contents in a receiver using the key contained there.
[0081]According to DTCPthe initial value of a key and the flag showing the changing timing of a key used for encryption of digital contents are correctly included in enciphered content. And at a receiverby changing too the initial value of the key contained in the enciphered content in the timing of the flag contained in the enciphered contentthe key used for encryption is generated and enciphered content is decoded. Howeverif the key for performing the decoding to enciphered content is containedeven if it will think that it is equivalentin order not to interferebelowit shall think such here. In the Web page specified by URL (Uniform Resource Locator) of http://www.dtcp.com about DTCP herefor exampleAcquisition of an informational version (Informational Version) is possible.
[0082]Nextthe contents of the analog signal from the outside are explained about the processing in the case of recording on the recording medium 195 according to the flow chart of drawing 3 (B). When the contents (analog content) of an analog signal are supplied to input-and-output I/F140input-and-output I/F140In Step S321the analog content is receivedan A/D conversion is carried out by A/D and D/A converter 141 which are followed and built in Step S322and it is considered as the contents (digital contents) of a digital signal.
[0083]These digital contents are supplied to the MPEG codec 130and in Step S323coding processing by MPEG encodingi.e.MPEG compressionis performedand they are supplied to the cipher-processing means 150 via the bus 110.
[0084]Hereafterin step SS324S325and S326processing in Step S302 of drawing 3 (A) and S303 and same processing are performed. That isATS addition to the transport packet by TS processing means 300 and encryption processing in the cipher-processing means 150 are performedthe enciphered content obtained as a result is recorded on the recording medium 195and recording processing is ended.
[0085]Nextthe contents recorded on the recording medium 195 are reproducedand the processing outputted as digital contents or analog content is explained according to the flow of drawing 4. Processing outputted outside as digital contents is performed as regeneration according to the flow chart of drawing 4 (A). That isfirstin Step S401the enciphered content recorded on the recording medium 195 is read by the drive 190 or recording-medium I/F210and it is outputted to the cipher-processing means 150 via the bus 110.
[0086]In the cipher-processing means 150in Step S402decoding processing of the

enciphered content supplied from drive 190 or recording-medium I/F210 is carried outand decode data is outputted to TS processing means 300 via the bus 110.
[0087]In Step S403TS processing means 300 judges output timing from ATS of each transport packet which constitutes a transport streamperforms control according to ATSand supplies it to input-and-output I/F120 via the bus 110. Input-and-output I/F120 outputs the digital contents from TS processing means 300 outsideand ends regeneration. Processing of TS processing means 300 and the decoding processing of the digital contents in the cipher-processing means 150 are mentioned later.
[0088]In input-and-output I/F120 being Step S404 and outputting digital contents via an IEEE1394 serial busBased on the standard of DTCPas mentioned aboveit attests mutually between a partner's devicesand digital contents are enciphered and transmitted after that.
[0089]When reproducing the contents recorded on the recording medium 195 and outputting outside as analog contentregeneration according to the flow chart of drawing 4 (B) is performed.
[0090]Namelyin Step S421S422and S423the respectively same processing as the case in Step S401 of drawing 4 (A)S402and S403 is performedand by thisThe decoded digital contents which were obtained in the cipher-processing means 150 are supplied to the MPEG codec 130 via the bus 110.
[0091]In the MPEG codec 130in Step S424MPEG decodingi.e.elongation processingis executed and digital contents are supplied to input-and-output I/F140. In Step S424D/A conversion (S425) of the digital contents by which MPEG decoding was carried out by the MPEG codec 130 is carried out by A/D and D/A converter 141 to build inand input-and-output I/F140 makes them analog content. And it progresses to Step S426and input-and-output I/F140 outputs the analog content outsideand ends regeneration.
[0092][Data format] Nextthe data format on the recording medium in this invention is explained using drawing 5. The minimum unit of reading and writing of the data on the recording medium in this invention is called by the name of the block (block). 1 block has 192*X (X) byte's (for exampleX= 32) size.
[0093]In this inventionATS is added to TS (transport stream) packet (188 bytes) of MPEG 2and as 192 bytesX of them are collected and it is considered as 1-block data. ATS is data in which 24 thru/or 32-bit mail arrival time is shownand as explained also in advanceit is the abbreviation for Arrival Time Stamp (mail arrival time stamp). ATS is constituted as data with the random nature according to the mail arrival time of each packet. X individual record of the TS (transport stream) packet which added ATS to one block (sector) of a recording medium is carried out. In the composition of this inventionthe block key which enciphers the data of the block (sector) using ATS added to the 1st TS packet of each block which constitutes a transport stream is generated.
[0094]By generating the block key for encryption using ATS with random naturea different inherent key for every block is generated. Encryption processing for every block is performed using the generated block inherent key. By having

composition which generates a block key using ATSthe field on the recording medium for storing the enciphering key for every block becomes unnecessaryand a main data area becomes usable effectively. It becomes unnecessary to access any data other than a main data division at the time of record of dataand reproductionand processing becomes efficient.
[0095]Block seed (Block Seed) shown in drawing 5 is the additional information containing ATS. Block seed is good also as composition which not only ATS but copy control information (CCI:Copy Control Information) added further. In this caseit can have composition which generates a block key using ATS and CCI.
[0096]Although the latter part explains the copy limit information (CCI:Copy Control Information) included in block seedhereIt is the copy control information (CCI:Copy Control Information) advocated by 5CDTCP (Digital Transmission Content Protection) system as a joint proposal of five companies.
Two kinds of information according to the capability of the devicei.e.EMI (Encyrption Mode Indicator)Or it becomes a thing reflecting one information of the embedding CCI (Embedded CCI) which is the copy control information (CCI) embedded to the contents applied in the format that the place for sending copy control information is secured beforehand.

[0097]In the composition of this inventionwhen it stores data on recording mediasuch as DVDthe data of most contents is encipheredbut. As shown in the bottom of drawing 5m (for examplem= 8 or 16) byte of the head of a block is recorded with a plaintext (Unencrypted data)without being encipheredand the remaining data (m+1 byte or subsequent ones) is enciphered. This is for restrictions to occur in cipher-processing data length (Encrypted data)since cipher processing is processing as an 8-byte unit. If cipher processing can carry out for example not per 8-byte unit but per byteall portions other than block seed may be enciphered as m= 4.
[0098][Processing in TS processing means] Herethe function of ATS is explained in detail. ATS is a mail arrival time stamp added since the appearance timing of each transport packet in an input transport stream is saved as explained also in advance.
[0099]Namelywhen one or some TV programs (contents) are taken out out of the transport stream which two or more TV programs (contents) multiplexedfor exampleThe transport packet which constitutes the taken-out transport stream appears at an irregular interval (refer to drawing 7 (a)). A transport stream has a meaning important for the appearance timing of each transport packetIt is determined at the time of coding that this timing will not ruin T-STD (Transport stream System Target Decoder) which is the virtual decoder specified with MPEG 2 systems (ISO/IEC 13818-1).
[0100]Appearance timing is controlled by ATS added to each transport packet at the time of reproduction of a transport stream. Thereforein recording a transport packet on a recording medium. When it is necessary to save the input timing of a transport packet and a transport packet is recorded on recording mediasuch as

DVDATS showing the input timing of each transport packet is added and recorded.
[0101]The block diagram explaining the processing which performs the transport stream inputted via a digital interface in TS processing means 300 when recording on the storage medium which are recording mediasuch as DVDis shown in drawing 6. From the terminal 600a transport stream is inputted as digital datasuch as digital broadcasting. In drawing 1 or drawing 2a transport stream is inputted from the terminal 600 via input-and-output I/F140 and the MPEG codec 130 via input-and-output I/F120.
[0102]A transport stream is inputted into the bit stream purser (parser) 602. The bit stream purser 602 detects an PCR (Program Clock Reference) packet out of an input transport stream. Herean PCR packet is a packet by which PCR specified with MPEG 2 systems is coded. The PCR packet is coded with the time interval of less than 100 msec. PCR expresses with the accuracy of 27 MHz the time when a transport packet reaches a receiver.
[0103]And PCR of a transport stream is made to carry out lock (Lock) of the 27 MHz clocks which a record reproducer has in 27MHzPLL603. The time stamp generation circuit 604 generates the time stamp based on the counted value of the clock of 27 MHz clocks. And the block seed (Block seed) additional circuit 605 is added to the transport packet by setting a time stamp in case the 1st byte of a transport packet is inputted into the smoothing buffer 606 to ATS.
[0104]The transport packet to which ATS was addedIt passes along the smoothing buffer 606and after cipher processing which it is outputted to the cipher-processing means 150and is explained in the latter part from the terminal 607 is performedit is recorded on the recording medium 195 which is a storage medium via the drive 190 (drawing 1) and recording-medium I/F210 (drawing 2).
[0105]Drawing 7 shows the example of processing in case an input transport stream is recorded on a recording medium. Drawing 7 (a) shows the input of the transport packet which constitutes a certain specific program (contents). A horizontal axis is a time-axis which shows the time on a stream here. In this examplethe input of a transport packet appears to irregular timingas shown in drawing 7 (a).
[0106]Drawing 7 (b) shows the output of the block seed (Block Seed) additional circuit 605. The block seed (Block Seed) additional circuit 605 adds the block seed (Block Seed) containing ATS which shows the time on the stream of the packet for every transport packetand outputs a source packet. Drawing 7 (c) shows the source packet recorded on the recording medium. As shown in drawing 7 (c)a source packet packs an interval and is recorded on a recording medium. Thusthe record section of a recording medium can be effectively used by packing and recording an interval.
[0107]Drawing 8 shows the processing constitution block diagram of TS processing means 300 in the case of reproducing the transport stream recorded on the recording medium 195. The transport packet with ATS decoded in a cipher-processing means to explain in the latter part is inputted into the block seed (Block seed) separation circuits 801and ATS and a transport packet are separated

from the terminal 800. The timing generating circuit 804 calculates the time based on the clock counter value of 27 MHz clocks 805 which a regenerator has.
[0108]Very first ATS is set to the timing generating circuit 804 as an initial value at the time of a reproductive start. The comparator 803 compares the present time inputted from ATS and the timing generating circuit 804. And when time for the timing generating circuit 804 to occur and ATS become equalthe output controlling circuit 802 outputs the transport packet to the MPEG codec 130 or digital-input/output I/F120.
[0109]Drawing 9 carries out MPEG encoding of the input AV signal in the MPEG codec 130 of the record reproducer 100and shows the composition which codes a transport stream in TS processing means 300 further. thereforedrawing 9 -- drawing 1 or drawing 2 -- it is a block diagram showing both the processing constitution of the MPEG codec 130 and TS processing means 300 to kick collectively. The video signal is inputted from the terminal 901 and it is inputted into MPEG video encoder 902.
[0110]MPEG video encoder 902 codes an input video signal to an MPEG video streamand outputs it to the buffer video stream buffer 903. MPEG video encoder 902 outputs the access unit information about an MPEG video stream to the multiplexing scheduler 908. The access unit of a video stream is a picture and access unit information is a picture type of each picturean encoding bit amountand a decoding time stamp. Herea picture type is the information on I/P/B picture (picture). A decoding time stamp is information specified with MPEG 2 systems.
[0111]The audio signal is inputted from the terminal 904 and it is inputted into MPEG audio encoder 905. MPEG audio encoder 905 codes an input audio signal to an MPEG audio streamand outputs it to the buffer 906. MPEG audio encoder 905 outputs the access unit information about an MPEG audio stream to the multiplexing scheduler 908. The access unit of an audio stream is an audio frameand access unit information is an encoding bit amount of each audio frameand a decoding time stamp.
[0112]The access unit information of video and an audio is inputted into the multiplexing scheduler 908. The multiplexing scheduler 908 controls the method of coding a video stream and an audio stream to a transport packet based on access unit information. As the multiplexing scheduler 908 has a clock which generates the reference time of 27-MHz accuracy in an inside and fills T-STD which is the virtual decoder model specified by MPEG 2it determines the packet encoding control information of a transport packet. Packet encoding control information is the kind of stream and the length of a stream which are packet-ized.
[0113]When packet encoding control information is a video packetit is on the a sidethe video data of payload-data length directed by packet encoding control information is read from the video stream buffer 903and the switch 976 is inputted into the transport packet coding equipment 909.
[0114]When packet encoding control information is an audio packetit is on the b sidethe audio information of payload-data length directed from the audio stream buffer 906 is readand the switch 976 is inputted into the transport packet coding

equipment 909.
[0115]When packet encoding control information is an PCR packetthe transport packet coding equipment 909 incorporates PCR inputted from the multiplexing scheduler 908and outputs an PCR packet. Nothing is inputted into the transport packet coding equipment 909 when directing that packet encoding control information does not code a packet.
[0116]The transport packet coding equipment 909 does not output a transport packetwhen directing that packet encoding control information does not code a packet. When othera transport packet is generated and outputted based on packet encoding control information. Thereforethe transport packet coding equipment 909 outputs a transport packet intermittently. The arrival (Arrival) time stamp (time stamp) calculating means 910 calculates ATS which shows the time when the 1st byte of a transport packet reaches a receiver based on PCR inputted from the multiplexing scheduler 908.
[0117]Since PCR inputted from the multiplexing scheduler 908 shows the arrival time to the 10th byte of receiver of the transport packet specified by MPEG 2the value of ATS serves as time when the byte 10 bytes before the time of PCR arrives.
[0118]The block seed (Block Seed) additional circuit 911 adds ATS to the transport packet outputted from the transport packet coding equipment 909. The transport packet with ATS outputted from the block seed (Block seed) additional circuit 911It passes along the smoothing buffer 912a cipher-processing means 150 HE input is carried outand it is stored in the recording medium 195 which is a storage medium after cipher processing explained in the latter part is performed.
[0119]Before being enciphered by the cipher-processing means 150the transport packet with ATS stored in the recording medium 195 is inputted where an interval is packedas shown in drawing 7 (c)and it is stored in the recording medium 195 after that. Even if a transport packet packs an interval and is recordedthe input time to the receiver of the transport packet is controllable by referring to ATS.
[0120]By the waythe size of ATS was not necessarily decided as 32 bitsand 24 bits thru/or 31 bits of it may be sufficient. The cycle around which the time counter of ATS goes becomes longso that the bit length of ATS is long. For examplewhen ATS is a binary counter of 27-MHz accuracytime for ATS of 24-bit length to go around is about 0.6 second. This time interval is size sufficient in a general transport stream. It is because the packet interval of the transport stream is decided to be a maximum of 0.1 second by regulation of MPEG 2. Howeversufficient margin is seen and it is good as for more than 24-bit in ATS.
[0121]Thuswhen bit length of ATS is made into various lengthsome composition is attained as composition of the block seed who is attached data of block data. Block seed's example of composition is shown in drawing 10. Example 1 of drawing 10 is an example which uses ATS by 32 bits. Example 2 of drawing 10 is an example which makes ATS 30 bits and uses copy control information (CCI) by 2 bits. Copy control information is information showing the state of copy-of-data control where it was added.

SCMS:Serial Copy Management System and CGMS:Copy Generation Management System are famous.
Copy free (Copy Free) which shows that the copy is permitted without restriction in such copy control information as for the data in which the information was addedInformationincluding the copy prohibition (Copy Prohibited) etc. which do not accept the one-generation copy permission (One Generation Copy Allowed) which permits the copy of only one generationand a copycan be expressed.
[0122]Example 3 shown in drawing 10 is an example which makes ATS 24 bitsuses 2 bits of CCI(s)and uses 6 bits of information of further others. As other informationwhen the analog output of this data is carried outfor exampleit is possible to use various informationincluding information etc.which shows ON and OFF (On/Off) of the macro vision (Macrovision) which is a copy control mechanism of an analog video data.
[0123][Tree (Thurs.) structure as key distribution composition] Nextthe composition which distributes the master key which needs it when the recording and reproducing device shown in drawing 1 or drawing 2 reproduces data from record or a recording medium to a recording medium to each apparatus is explained. Drawing 11 is a figure showing the distribution composition of the key of the recording and reproducing device in the recording system which used this method. The numbers 0-15 shown in the bottom of drawing 11 are each recording and reproducing devices. That iseach leaf (leaf: leaf) of the tree (tree) structure shown in drawing 11 is equivalent to each recording and reproducing device.
[0124]Each devices 0-15 store in person the key (node key) assigned to the node of a to [from its own leaf in the initial tree defined beforehand / a route]and the leaf key of each leaf at the time of manufacture (at the time of shipment). K0000-K1111 which are shown in the bottom of drawing 11 are the leaf key assigned to each devices 0-15respectivelyand let key:KR-K111 indicated in the 2nd paragraph (node) from the bottom be a node key from KR of the highest rung.
[0125]In the tree composition shown in drawing 11the device 0 owns the leaf key K0000node key:K000 and K00K0and KR. The device 5K0101K010K01K0and KR are owned. The device 15 owns K1111K111K11K1and KR. Although 16 devices of 0-15 are indicated to the tree of drawing 11 and the tree structure is also shown as symmetrical composition which was able to take balance of 4 stage constitutionit is possible to have number-of-stages composition which much more devices are constituted in a treeand is different in each part of a tree.
[0126]The record reproducer various type which uses various recording mediafor exampleDVDCDMDa memory stick (trademark)etc. is contained in each record reproducer contained in the tree structure of drawing 11. It is assumed that various application services live together. The key distribution composition shown in drawing 11 after such a different device and different application constitute [coexistence] is applied.
[0127]In the system by which these various devices and application live togetherthe portion 012and 3 enclosed with the dotted line of drawing 11i.e.devicesis set up as one group using the same recording medium. For

examplethe device contained in the group enclosed with this dotted line is receivedIt collectsand common contents are enciphered and processing in which send the master key which is sent from a provider or is used in commonor encipher to a provider or a settlement-of-accounts organization tooand the payment data of a content rate is outputted to it from each device is performed. Organizations which perform data transmission and reception with each devicesuch as a content provider or a settlement processing organizationperform the portion enclosed with the dotted line of drawing 11i.e.the processing which bundle up the devices 012and 3 as one groupand sends data. Two or more such groups exist in the tree of drawing 11.

[0128]A node key and a leaf key are good also as composition managed for every group with the provider who may generalize and manage by one certain lock management centerand performs various data transmission and reception to each groupa settlement-of-accounts organizationetc. As for these node keys and a leaf keyin disclosure of a keyetc.an update process is performedand a lock management centera providera settlement-of-accounts organizationetc. perform this update process.

[0129]In this tree structurethe three devices 012and 3 contained in one group hold the key K00 common as a node keyK0and KR so that clearly from drawing 11. By using this node key share compositionit becomes possible to provide only the devices 012and 3 with a common master keyfor example. For exampleif node key K00 the very thing held in common is set up as a master keysetting out of a master key only with the common devices 012and 3 is possiblewithout performing new key sending. If the value Enc (K00Kmaster) which enciphered the new master key Kmaster by the node key K00 is stored in a recording medium via a network and distributed to the devices 012and 3Only the devices 012and 3 become possible [solving the code Enc (K00 Kmaster) using the share node key K00 held in each deviceand obtaining master key:Kmaster]. It is shown that Enc (KaKb) is the data which enciphered Kb by Ka.

[0130]When it is revealed in t at a certain time that key:K0011 which the device 3 ownsK001K00K0and KR were analyzed by the aggressor (hacker)and it was exposed of KRAfter itin order to protect the data transmitted and received by a system (group of the devices 012and 3)it is necessary to separate the device 3 from a system. for that purpose -- a node key -- : -- K -- 001 -- K -- 00 -- K -- zero -- KR -- respectively -- being new -- a key -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- updating -- a device -- zero -- one -- two -- the -- updating -- a key -- it is necessary to tell . Hereit is shown that K(t) aaa is an updating key of generation (Generation):t of the key Kaaa.

[0131]distribution **** of an updating key -- it ****** just. The renewal of a key the table constituted by the block data called the validation key blocks (EKB:Enabling Key Block) shown in drawing 12 (A)for example For examplea networkOr it performs by storing in a recording medium and supplying the devices 01and 2.

[0132]It is constituted as block data which has a data configuration which can update only the required device of renewal of a node key in the validation key blocks (EKB) shown in drawing 12 (A). In the devices 01and 2 in the tree structure shown in drawing 11the example of drawing 12 is the block data formed for the purpose of distributing the generation's t updating node key. drawing 11 -- from -- being clear -- as -- a device -- zero -- a device -- one -- updating -- a node key -- ****** -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- required -- a device -- two -- updating -- a node key -- ****** -- K -- (-- t --) -- 001 -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- being required .

[0133]As shown in EKB of drawing 12 (A)two or more cryptographic keys are contained in EKB. The cryptographic key of the bottom is Enc (K0010K(t)001). this -- a device -- two -- having -- a leaf key -- K -- 0010 -- enciphering -- having had -- updating -- a node key -- K -- (-- t --) -- 001 -- it is -- a device -- two -- self -- having -- a leaf key -- this -- a cryptographic key -- decoding -- K -- (-- t --) -- 001 -- it can obtain . using K(t)001 obtained by decodingdecoding of the 2nd step of cryptographic key Enc (K -- (-- t --) -- 001 -- K -- (-- t --) -- 00) is attained from under drawing 12 (A)and updating node key K(t)00 can be obtained. belowone by onethe 2nd step of cryptographic key Enc (K -- (-- t --) -- 00 -- K -- (-- t --) -- 0) is decoded from on drawing 12 (A)the 1st step of cryptographic key Enc (K(t) 0 and K (t) R) is decoded from on updating node key K(t)0 and drawing 12 (A)and K(t) R is obtained. on the other hand -- a device -- zero -- one -- a node key -- K -- 000 -- updating -- an object -- containing -- not having -- updating -- a node key -- ****** -- being required -- a thing -- K -- (-- t --) -- 00 -- K -- (-- t --) -- zero -- K -- (-- t --) -- R -- it is . The devices 0 and 1 decode the 3rd step of cryptographic key Enc (K000K(t)00) from on drawing 12 (A)and acquire K(t)00hereafterthe 2nd step of cryptographic key Enc (K -- (-- t --) -- 00 -- K -- (-- t --) -- 0) is decoded from on drawing 12 (A)the 1st step of cryptographic key Enc (K(t) 0 and K (t) R) is decoded from on updating node key K(t)0 and drawing 12 (A)and K(t) R is obtained. Thusthe devices 01and 2 can obtain updated key K(t) R. The index of drawing 12 (A) shows the actual address of the node key and leaf key which are used as a decryption key.

[0134]The node key of the upper stage of the tree structure shown in drawing 11 : when renewal of K0 and KR is unnecessary and the update process of only the node key K00 is requiredBy using the validation key blocks (EKB:Enabling Key Block) of drawing 12 (B)updating node key K(t)00 can be distributed to the devices 01and 2.

[0135]EKB shown in drawing 12 (B) is available when distributing the new master key sharedfor example in a specific group. As an examplethe recording medium with the devices 012and 3 in the group who shows by a dotted line is used for drawing 11and suppose that new common master key K(t) master is required. this -- the time -- a device -- zero -- one -- two -- three -- being common -- a node key -- K -- 00 -- having updated -- K -- (-- t --) -- 00 -- using -- being new -- being common -- updating -- a master key -- : -- K -- (-- t --) --

master -- having enciphered -- data -- Enc (K (t)K(t) master) -- drawing 12 -- (-- B --) -- being shown -- EKB -- distributing . By this distributionthe distribution as data of the device 4 etc. which is not decoded in other groups' apparatus is attained.

[0136]That isif the devices 01and 2 decode the above-mentioned cryptogram using K(t)00 which processed and obtained EKBit will become possible to obtain master key K(t) master in t time.

[0137][Distribution of the master key which uses EKB] as an example of processing which obtains master key K(t) master in t time to drawing 13K (t) Processing of the device 0 which received EKB shown in the data Enc (K(t) 00 and K (t) master) which enciphered new common master key K(t) master using 00and drawing 12 (B) via the recording medium is shown.

[0138]As shown in drawing 13the device 0 generates node key K(t)00 by same EKB processing with having mentioned above using the node key K000 which EKB and the them at the generation:t time stored in the recording medium store beforehand. Updating master key K(t) master is decoded using updating node key K(t)00 decodedand in order to use it behindit enciphers and stores by the leaf key K0000 which he has. When the device 0 can store updating master key K(t) master in self safelyit is not necessary to encipher by the leaf key K0000.

[0139]The flow chart of drawing 14 explains the acquisition processing of this updating master key. The recording and reproducing device can give the master key:K(c) master newest in the time at the time of shipmentand assumes that it stores in an own memory safely (specifically enciphering by an own leaf key).

[0140]When the recording medium with which updating master key K(n) master and EKB were stored is set in a recording and reproducing devicein Step S1401first a recording and reproducing deviceNumber:n (this is made to call it pre (pre-recording) record generation information (Generation#n)) is read from a recording medium at the time (generation) of master key K(n) master stored in the recording medium. Number:n is beforehand memorized by the recording medium at the time (generation) of master key K(n) master. The encryption master key C which self holds is readgeneration:c of the encryption master key is compared with generation:n which pre record generation information Generation#n expresses in Step S1402and the generation order is judged.

[0141]In Step S1402the direction which is generation:n which pre record generation information Generation#n expressesWhen judged with it not being backward (it is not new) rather than generation:c of the encryption master key C memorized by the own memoryThat isas that of generation:n which pre record generation information Generation#n expressesor in a next casegeneration:c of the encryption master key C memorized by the memory skips Steps S1403 thru/or S1408and ends a master key update process. That issince it is not necessary to perform renewal of master key K(c) master (encryption master key C) memorized by the own memory in this casethat updating is not performed.

[0142]On the other hand in Step S1402the direction which is generation:n which pre record generation information Generation#n expressesWhen judged with it

being the back [c / of the encryption master key C memorized by the memory / generation:] (new)Namelywhen the generation of the encryption master key C memorized by the memory is a generation before the generation n whom pre record generation information Generation#n expressesProgressing to Step S1403a recording and reproducing device reads validation key blocks (EKB:Enabling Key Block) from a recording medium.

[0143]In Step S1404a recording and reproducing deviceEKB read at Step S1403and the leaf key (K0000 in the device 0 of drawing 11) and node key (K000 in the device 0 of drawing 11K00 ...) which self stores in a memory are usedKey K(t)00 of the node 00 in a pre record generation information Generation#n (t in drawing 13) time are calculated.

[0144]In Step S1405it is inspected whether K(t)00 were able to be obtained in Step S1404. Since it is shown that RIBOKU (exclusion) of the recording and reproducing device is done at the time by the group of tree composition when not obtainedSteps S1406 thru/or S1408 are skippedand a master key update process is ended.

[0145]K (t) When 00 is able to be obtainedit progresses to Step S1406 and Enc (K(t) 00 and K (t) master)i.e.the value which enciphered the master key in t time using K(t)00is read from a recording medium. And in Step S1407K(t) master is calculated by decoding this cryptogram using K(t)00.

[0146]In Step S1408K(t) master is enciphered using the leaf key (K0000 in the device 0 of drawing 11) which only self hasand it stores in a memory. Abovethe update process of a master key is completed.

[0147]By the wayalthough the master key is used for the ascending order from the time (generation) 0it is desirable to have composition with which each apparatus in a system is asked for an old generation's master key by calculation from a new generation's master key. That ison the other handthe recording and reproducing device holds the tropism function f.

When only the number of times corresponding to the difference of the generation of the master key and the generation of a required master key applies the master key which self has in the tropism function f on the other handthe master key of the generation who investigated is created.

[0148]The generation of the master key MK memorized by the recording and reproducing device is specifically the generation i+1for exampleWhen the generation of the master key MK required (used at the time of record) for reproduction of a certain data is the generation i-1master key K(i-1) masterIn a recording and reproducing deviceon the other handthe tropism function f is used twice and generated by calculating f (f (K(i+1) master)).

[0149]When the generation of the master key memorized by the recording and reproducing device is the generation i+1 and the generation of a required master key is the generation i-2master key K(i-2) masterOn the other handit is generated by calculating f (f (f (K(i+1) master)))using the tropism function f 3 times.

[0150]Hereon the other hand as a tropism functiona hash (hash) function can be

usedfor example. SpecificallyMD5 (Message Digest 5)SHA-1 (Secure Hash Algorithm - 1)etc. are employablefor example. master key K(0) master in whichas for the key issuing agency which publishes a keyself can generate the generation before a generation using these one-way nature functionsK(1) masterand K(2) master ... and K(N) master are calculated beforehand. By namelythe thing which master key K(N) master of the Nth generation is set upa tropism function is first applied to master key K(N) master 1 time respectively on the other handand it goes. Master key K(N-1) master of the generation before itK(N-2) master...K(1) masterand K(0) master are generated one by one. And it is used in an order from a generation's small master key K(0) master (before). On the other handlet a tropism function be the thing which is used for generating the master key of the generation before an own generation and which is set as all the recording and reproducing devices.

[0151]It is also possible toadopt public-key-encryption art as a tropism function on the other handfor example. In this casea key issuing agency owns the secret key of a public-key crypto systemand gives the public key to that secret key to all the playback equipment. And a key issuing agency sets up master key K(0) master of the 0th generationand uses it from master key K(0) master. That isa key issuing agency will generate and use master key K(i-1) master in front of one of them by changing with a secret keyif master key K(i)master after the 1st generation is needed. In this caseon the other handthe key issuing agency does not need to generate Generation N's master key beforehand using a tropism function. According to this methodthe theory top can generate an unrestricted generation's master key. In a recording and reproducing deviceif it has a certain generation's master keythe master key of the generation before the generation can be obtained by changing the master key by a public key.

[0152]Nextprocessing of a recording and reproducing device in case this recording and reproducing device records contents on an own recording medium is explained using the flow chart of drawing 15. It is enciphered with a certain generation's master keyand contents data is distributed to each recording and reproducing device from contents pro BAITA via a network or a recording medium.

[0153]Firstin Step S1501a recording and reproducing device reads pre record generation information Generation#n from a recording medium. The generation c of the encryption master key C which the own memory has memorized is acquiredthe generation c of the encryption master key is compared with the generation n whom pre record generation information Generation#n expresses in Step S1502and the generation order is judged.

[0154]In Step S1502the generation c of the encryption master key C memorized by the memory. When judged with it not being after the generation n whom pre record generation information Generation#n expressesThat iswhen the generation c of the encryption master key C memorized by the memory is a generation older than the generation n whom pre record generation information Generation#n expressesit endswithout skipping Step S1503namelyperforming recording processing of contents data.

[0155]On the other hand in Step S1502the generation of the encryption master key C memorized by the memory in an own recording and reproducing deviceWhen judged with it being after the generation n whom pre record generation information Generation#n expressesThat isas that of the generation n whom pre record generation information Generation#n expressesor when newer than itthe generation of the encryption master key C memorized by the memory progresses to Step S1503and performs recording processing of contents data.
[0156][Contents data encryption with the master key in which generation management was made and recording processing] Contents data encryption processing is hereafter performed with the master key in which generation management was madeand the processing stored in a self recording medium is explained. Herethe processing which generates a block key based on the data using the master key by which generation management was carried out in the data constituted by the transport stream explained previouslyenciphers contents data with a block keyand is stored in a recording medium is explained.
[0157]It explains using drawing 16the processing block figure of drawing 17and the flow chart of drawing 18. Herelet an optical disc be an example as a recording medium. In order to prevent the bit-by-bit copy of the data on a recording mediumhe is trying to make disk ID (Disc ID) as identification information peculiar to a recording medium act on the key which enciphers data in this working example.
[0158]According to the processing block figure of drawing 16 and drawing 17the outline of encryption processing of the data which the cipher-processing means 150 performs is explained.
[0159]The master key 1601the key 1631 for data analysis recording methods (cog NIZANTOKI: Cognizant Key)or the key for data non-analyzing recording methods (non cog NIZANTOKI:.) which stores the recording and reproducing device 1600 in the own memory 180 (drawing 1two references) Non-Cognizant Key1632 is read. The key for data analysis recording methods (Cognizant Key) and the key for data non-analyzing recording methods (Non-Cognizant Key) are mentioned later.
[0160]The master key 1601 is the secret key stored in the memory of a recording and reproducing device by the flow of drawing 14.
Generation management is made as mentioned above and the generation number is matched with each.
This master key is a key common to two or more recording and reproducing devicesfor examplea key common to the device belonging to the group of a dotted-line frame who shows drawing 11. The device ID is an identifier of the recording and reproducing device 1600and for exampleit is beforehand stored in the recording and reproducing devicethey are identifierssuch as a serial number. This device ID may be exhibited. The key 1631 for data analysis recording methods (Cognizant Key) and the key 1632 for data non-analyzing recording methods (Non-Cognizant Key) are keys corresponding to each recording mode.
It is a key common to two or more recording and reproducing devices.
These are beforehand stored in the memory of the recording and reproducing

device 1600.
[0161]It is inspected whether as for the recording and reproducing device 1600disk ID(Disc ID) 1603 as identification information is already recorded on the recording medium 1620 which is an optical disc. If are recordedand disk ID(Disc ID) 1603 is read (equivalent to drawing 16) and it is not recordedFor exampleit was set at random or beforehand in the cipher-processing means 150disk ID(Disc ID) 1701 is generated by methodssuch as a random number generationand it records on a disk (equivalent to drawing 17). The thing with one stored in read in area etc. since it is good is also possible for disk ID(Disc ID) 1603 on the disk.
[0162]Stamper ID(Stamper ID) 1680 on which the record reproducer 1600 was recorded from the disk only by the master key and the special method of reading next as confidential information which can be readA disk inherent key (Disc Unique Key) is carried out generation 1602 using disk ID1603.
[0163]As a concrete generation method of a disk inherent key (Disc Unique Key)using a master keystamper ID(Stamper ID) 1680 as confidential informationand disk ID1603The method of Example 1 using the result obtained by inputting master key (Master Key)stamper ID (Stamper ID)and disk ID (Disc ID) into the hash function using a block cipher function as shown in drawing 19To hash function SHA-1 defined by FIPS 180-1. The data generated by the bit connection to a master keystamper ID (Stamper ID)and disk ID (Disc ID) is inputtedThe method of Example 2 which uses only required data length as a disk inherent key (Disc Unique Key) from the output of 160 bits is applicable.
[0164]As mentioned abovestamper ID(Stamper ID) 1680 is advanced confidential information currently beforehand recorded on the disk.
Data processingsuch as generation etc. of the disk inherent key (Disc Unique Key) using the read-out and read stamper ID (Stamper ID)is performed inside a cipher-processing means so that a secret may be maintained.
That isthe confidential information read from the disk is protected by secure one in a cipher-processing means.
[0165]Thusin the composition of this invention the confidential information which can be read only with a special read methodIt is read with a just devicei.e.the device which can perform how to read confidential informationFor exampleit is the composition used for the key generation processing for contents cipher processing under secure protection in the cipher-processing part which performs generation of the encryption key which was mounted in LSI and protected highlyand confidential information is not stored on the memory in which reading from the outside is possible. Thereforethere is no possibility of disclosure of confidential information and it becomes possible to prevent regeneration of inaccurate contents effectively.
[0166]As mentioned abovereading only in the technique of being written in a disk in a different mode from the usual data writing techniqueand being different from the usual data read is possible for confidential informationsuch as stamper ID. The latter part explains the writing and the example of reading processing composition of this confidential information in detail.

[0167]For exampletitle key (Title Key) which is an inherent key for every record was provided in the recording and reproducing device 1600 at random or beforehand in the cipher-processing means 150 (drawing 12reference) nextgeneration 1604 is taken by methodssuch as a random number generationand it is recorded on the disk 1620.
[0168]The recording mode in this record carries out the flag showing a data analysis recording method (Cognizant Mode)or data a non-analyzing recording method (Non-cognizant) setting-out 1633and records the recording mode 1635 on the disk 1620.
[0169]Herea data analysis recording method (Cognizant Mode)and data a non-analyzing recording method (Non-Cognizant Mode) are explained.
[0170]It s specified on what kind of conditions a contents provider can reproduce contents beforehandrespectively. Thenthere is the necessity of telling the specified condition correctly to a partner's apparatus also in network connectionIn 5C DTCP (Digital Transmission Content Protection) system as a joint proposal of five companiesit has solved using the method of copy control information (CCI:Copy Control Information). According to the capability of a devicetwo kinds of methods of communication are specified to copy control information (CCI).
[0171]An encryption mode indicator (EMI:Encyrption Mode Indicator) is a mechanism which sends copy control information (CCI) using top 2 bits of Sy bit in a packet headerSince a receiving device can access easilysimultaneously it acts on the key with which this value enciphers contentsit can send safely.
[0172]EMI shows the encryption mode of the packet and the generation mode of a contents code and a decode key is specified. By putting EMI on an IEEE1394 packet headerIt comes out of a receiver to get to know in which mode contents are enciphered simplywithout taking out the embedding copy control information (Embedded CCI) (after-mentioned) currently embedded in the MPEG transfer stream (MPEG transport stream).
[0173]An IEEE1394 packet format is shown in drawing 20. In data field (Data Field)Various contentssuch as music data and image dataare storedThe encryption mode indicator (EMI:Encryption Mode Indicator) as copy control information (CCI) is set as top 2 bits of Sy bit in a packet header.
[0174]2 bit information of EMI specifies the handling from which contents differ according to a preset value. Attestation and encryption of the value 00 are unnecessaryand contents specifically show copy free (Copy Free) which can be copied freelyCreation of a time cost copy is possible for the value 01. Copy 1 generation (Copy One Generation)The value 11 expresses the NEBA copy (Never Copy) whose contents are copy prohibition from a release point in time about no more copy (No More Copies) to which the re-copy once Copy One Generation of the above-mentioned [the value 10] was recorded is forbidden.
[0175]So that works can be correctly dealt with also by a bit stream recorder which does not recognize the format of data like D-VHS or a hard disk recordedEmbed at the time of record and renewal of CCI (Embedded CCI) is not needed to from ex.Copy One Generation to No More CopiesThe record method

that what is necessary is to perform only renewal of EMI is data the recording method non-analyzing (Non-Cognizant).
[0176]In the format (for examplea DV format: DV-format) that on the other hand the place for sending such copy control information is secured beforehandCCI can be transmitted as some contents. Thusthe copy control information (CCI) embedded to contents as some contents is embeddedand it is referred to as CCI (Embedded CCI). Usuallywhen contents are enciphered and transmittedit is similarly enciphered as contentsthe embedding CCI (Embedded CCI) is also transmittedand a change of the intentionally of the embedding CCI (Embedded CCI) is made difficult.
[0177]In the case of the contents which have here the both sides of the 2-bit copy control information of EMI mentioned aboveand the embedding CCI (Embedded CCI). A certain storage device which performs contents recording updates the copy control information of the both sides of EMI and the embedding CCI (Embedded CCI). Howeverin the case of a storage device without the analysis capability of the embedding CCI (Embedded CCI)EMI updatesbut renewal of the embedding CCI (Embedded CCI) will be performed.
[0178]At the time of contents recordingthe recording method which a storage device updates the embedding CCI (Embedded CCI) transmitted as some contentsand records with contents is called data analysis (Cognizant) recording method. In a data analysis (Cognizant) recording methodand data the recording method non-analyzing (Non-Cognizant). Although it is easy to mount the part and load which the direction of data the recording method non-analyzing (Non-Cognizant) does not need to embedand do not need to update CCI (Embedded CCI) lightlyas a rule of 5CDTCPIn order for the apparatus to carry out MPEG decoding of the contents and to display a video signal from an analog terminalthe apparatus has the rule that it must be a data analysis recording method (Cognizant Mode)The apparatus with decoding/display function needs to have the function to perform a data analysis recording method (Cognizant Mode).
[0179]Howeverin order to perform a data analysis recording method (Cognizant Mode)againIt is necessary to get to know thoroughly the position and meaning of the embedding CCI (Embedded CCI) which are embedded as some contents. For exampleit may become very difficult for old apparatus to perform a data analysis recording method (Cognizant Mode) to the new data format about the data format which was enacted after a certain apparatus came out to the commercial scene and which is new or was updated.
[0180]Thereforea certain apparatus which records contents about a specific data format. Or when realizing a specific functionperform a data analysis recording method (Cognizant Mode)and at the time of the contents recording of a different data format. It is possible to perform both recording methods of performing data a non-analyzing recording method (Non-Cognizant Mode).
[0181]The apparatus which performs only record of data a non-analyzing recording method (Non-CognizantMode) also exists to all the contents. It is possible that the apparatus which performs only processing with the format which embeds

conversely and can understand CCI (Embedded CCI) of contentsi.e.the apparatus which are data-analysis-recording-method(Cognizant Mode)-acceptedand is performedexists.
[0182]Thusalso as apparatus which it embeds with two copy control informationi.e.EMIand CCI (Embedded CCI) existsand performs contents recordingThe apparatus which performs a data analysis recording method (Cognizant Mode)In the situation where the apparatus which performs record of data a non-analyzing recording method (Non-Cognizant Mode) is intermingledAs for the contents recorded by the data analysis recording method (Cognizant Mode)and the contents recorded by the data non-analyzing recording method (Non-Cognizant Mode)being distinguished clearly is preferred.
[0183]Namelywhen contents are recorded by a data analysis recording method (Cognizant Mode)also embed EMI and the copy control information of the both sides of CCI (Embedded CCI) is updatedbut. When record of contents is performed by data a non-analyzing recording method (Non-Cognizant Mode)only EMI is updated and renewal of the embedding CCI (Embedded CCI) is not performed. As a resultit is for confusion to ariseif it embeds with EMI on a recording mediummismatching starts to CCI (Embedded CCI) and the both are mixed. Thereforein order not to generate the mismatching of two copy control information. The contents recorded by the data analysis recording method (Cognizant Mode)Record reproduction processing with data analysis recording method (Cognizant Mode) mode is performedIt is necessary for the contents recorded by the data non-analyzing recording method (Non-Cognizant Mode) to have composition which performs record reproduction processing in data non-analyzing recording method (Non-Cognizant Mode) mode.
[0184]For the purposealthough it is also an idea to completely make this data analysis recording method (Cognizant Mode)and data a non-analyzing recording method (Non-Cognizant Mode) into another recording methodIn this casein order to enable execution of both modes selectively in one apparatusit is necessary to equip one apparatus with the executive operation composition in both the modesand this has the problem of causing the high cost of apparatus.
[0185]In the composition of this inventionthenthese two recording methods (Cognizant Mode)i.e.a data analysis recording methodBy having composition which uses the key for contents cipher processing generating it as a different key according to whether which method of data a non-analyzing recording method (Non-Cognizant Mode) is applied. According to apparatus and a recording methoddistinguish two recording methods clearlyand the situation where both methods are performed by being intermingled disorderly is canceledContents processing constitution by one [the gap which wants to respond to apparatus and a recording methodor] unific recording method is realized without increasing equipment of apparatus and a processing load.
[0186]Specifically The encryption as confidential information (required also at the time of reproduction) for data analysis recording method (Cognizant Mode) recordProvide only for apparatus with the function in which the record or

reproduction for decoding processing key generation according a key (key for data analysis recording methods (Cognizant Key)) to a data analysis recording method (Cognizant Mode) can be performedhave composition stored in apparatus and on the other handThe encryption as confidential information (required also at the time of reproduction) for data non-analyzing recording method (Non-Cognizant Mode) recordIt had composition with which only apparatus with the function in which the record or reproduction for decoding processing key generation according a key (key for data non-analyzing recording methods (Non-Cognizant Key)) to data a non-analyzing recording method (Non-Cognizant Mode) can be performed is provided and which is stored in apparatus.

[0187]By this compositionabout the contents recorded by the data analysis recording method (Cognizant Mode)for examplemake a bug into a cause and by or the alteration of dataunjust reconstruction of a record reproduction programetc. In the apparatus which has only a record reproduction function of data a non-analyzing recording method (Non-Cognizant Mode)execution of unjust record reproduction can be prevented accidentally.

[0188]It returns to drawing 16 and drawing 17and explanation of contents recording processing is continued. The recording and reproducing device 1600 acquires generation number [record times cost number (Generation#n)] 1650 of the master key which the generation number of the master key to be usedi.e.selfstores furtherand stores this in the recording medium 1620 as the record times cost number 1651.

[0189]On a diskthe data management file in which the information what data constituted what kind of title was stored isGeneration number [record times cost number (Generation#n)] 1651 of the title key 1605the record mode flag 1635and a master key are storable in this file.

[0190]The pre (pre-recording) generation number is beforehand stored in the recording medium 1620.

It has composition which enables reproduction of only the contents enciphered and stored using the master key of the same or generation newer than a pre generation number as a pre generation number.

The column of latter regeneration explains this composition.

[0191]Nexta disk inherent key (Disc Unique Key)title key (Title Key)and the key for data analysis recording methods (Cognizant Key)Or a disk inherent key (Disc Unique Key) and the title key (Title Key)A title inherent key (Title Unique Key) is generated from the key (Non-CognizantKey) for data non-analyzing recording methodsand one of combination.

[0192]Namelywhen a recording mode is a data analysis recording method (Cognizant Mode). A disk inherent key (Disc Unique Key) and the title key (Title Key)A title inherent key (Title Unique Key) is generated from the key for data analysis recording methods (Cognizant Key)When a recording mode is data a non-analyzing recording method (Non-Cognizant Mode)A title inherent key (Title Unique Key) is generated from a disk inherent key (Disc Unique Key)title key (TitleKey)and the key for data non-analyzing recording methods (Non-Cognizant

Key).
[0193]As mentioned abovethe encryption as confidential information for data analysis recording method (Cognizant Mode) recordThe key for decoding processing key generation (the key for data analysis recording methods (Cognizant Key)) Only apparatus with the function in which the record or reproduction by a data analysis recording method (Cognizant Mode) can be performed hasThe encryption as confidential information for data non-analyzing recording method (Non-Cognizant Mode) record on the other handThe key for decoding processing key generation (only apparatus with the function in which the record or reproduction by data a non-analyzing recording method (Non-Cognizant Mode) can be performed has a key for data non-analyzing recording methods (Non-Cognizant Key).) Thereforein the apparatus only corresponding to one recording methodonly one of the modes is chosen and contents recording is performed. That isit will be restricted only to one side of whether the key for data analysis recording methods (Cognizant Key) is usedor to use the key for data non-analyzing recording methods (Non-Cognizant Key).
[0194]Howeverboth key is stored and the processing which determines whether to perform record by which mode is needed in the apparatus which can perform the recording method in both the modes. . [whether record of this mode determination process treatmenti.e.contentsis performed by a data analysis recording method (Cognizant Mode)and] It is explained using drawing 21 whether it performs by data a non-analyzing recording method (Non-Cognizant Mode) about the process to determine.
[0195]Fundamentallyas for contents recordingit is desirable to perform by a data analysis recording method (CognizantMode) as much as possible. This is for embedding with EMI and not producing mismatching with CCI (Embedded CCI)as mentioned above. Howeveras mentioned abovethere are possibilities of generatingsuch as a data analysis error by the appearance of a new data formatetc.andin such a caserecording processing in data a non-analyzing recording method (Non-Cognizant Mode) is performed.
[0196]Each step of drawing 21 is explained. In Step S5001it is judged whether analysis of a data format is possible for a recorder. As explained previouslythe embedding CCI (Embedded CCI) is embedded to the inside of contents.
Since reading of the embedding CCI (Embedded CCI) will become impossible if the analysis of a data format is impossiblerecording processing in data a non-analyzing recording method (Non-Cognizant Mode) is performed in this case.

[0197]If the analysis of a data format is possibleit will progress to Step S5002 and a recorder will judge whether decoding of data (contents)reading of the embedding CCI (Embedded CCI)and an update process are possible. Contents and the embedding CCI (Embedded CCI) are usually coded (encoding)and it is necessary for reading of the embedding CCI (Embedded CCI) to perform decoding (decoding). For examplefor the Reasons of the decoder circuit being used otherwise in the casessuch as multi-channel simultaneous recordwhen decoding processing is not

possible for apparatusSince reading of the embedding CCI (Embedded CCI) cannot be performedrecording processing in data a non-analyzing recording method (Non-Cognizant Mode) is performed.
[0198]In [if judged with decoding of the data (contents) of Step S5002reading of the embedding CCI (Embedded CCI)and an update process being possible] Step S5003It is judged whether they are whether the run designation input of the recording processing in data non-solution mode is during the user input to a recorder and no. This processing is a step performed only in the apparatus which made mode select by a user's specification possible.
It does not perform in usual apparatusi.e.the apparatus which does not permit the mode specification by a user.
When there is recording processing specification by data the non-analyzing recording method by a user input (Non-Cognizant Mode)recording processing in data a non-analyzing recording method (Non-Cognizant Mode) is performed.
[0199]Nextin Step S5004it is judged whether the run designation of the recording processing in data non-solution mode occurs in a contents packet (ex. received data). When the run designation of the recording processing in data non-solution mode occurs in datarecording processing in data a non-analyzing recording method (Non-Cognizant Mode) is performed. When there is no specificationrecording processing in a data analysis recording method (Cognizant Mode) is performed.
[0200]The recording processing in a data analysis recording method (Cognizant Mode)And it is determined by the mode determination process treatment which mentioned above selectively the both sides of the recording processing in data a non-analyzing recording method (Non-Cognizant Mode) in the apparatus which can be performed whether record with which mode is performed. Howeverwhen record by a data analysis recording method (Cognizant Mode) is possibleprocessing by a data analysis recording method (Cognizant Mode) will be fundamentally performedso that I may be understood also from the process flow of drawing 21.
[0201]As mentioned abovewhen a recording mode is made into a data analysis recording method (Cognizant Mode)A disk inherent key (Disc Unique Key) and the title key (Title Key)A title inherent key (Title Unique Key) is generated from the key for data analysis recording methods (Cognizant Key)When a recording mode is made into data a non-analyzing recording method (Non-Cognizant Mode)A title inherent key (Title Unique Key) is generated from a disk inherent key (Disc Unique Key)title key (TitleKey)and the key for data non-analyzing recording methods (Non-Cognizant Key).
[0202]The concrete method of title inherent key (Title Unique Key) generation is shown in drawing 22. As shown in drawing 22to the hash function using a block cipher function Title key (Title Key) and a disk inherent key (Disc Unique Key)the key for data analysis recording methods (Cognizant Key) (in the case of a data analysis recording method (Cognizant Mode)) -- orThe method of Example 1 using the result obtained by inputting the key for data non-analyzing recording methods (Non-Cognizant Key) (in the case of data a non-analyzing recording method (Non-

Cognizant Mode))To hash function SHA-1 [or] defined by FIPS 180-1. A master keydisk ID (Disc ID)the key for data analysis recording methods (Cognizant Key) (in the case of a data analysis recording method (Cognizant Mode))or the key for data non-analyzing recording methods (Non-Cognizant.) The data generated by the bit connection to Key (in the case of data a non-analyzing recording method (Non-Cognizant Mode)) is inputtedThe method of Example 2 which uses only required data length as a title inherent key (Title Unique Key) from the output of 160 bits is applicable.

[0203]In the above-mentioned explanationa disk inherent key (Disc Unique Key) is generated from master key (Master Key)stamper ID (Stamper ID)and disk ID (Disc ID)A title inherent key (Title UniqueKey) from thistitle key (Title Key)the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key). Although he is trying to generaterespectivelyUsing a disk inherent key (Disc Unique Key) as unnecessary Master key (Master Key)disk ID (Disc ID)and the title key (TitleKey)A title inherent key (Title Unique Key) may be directly generated from the key for data analysis recording methods (Cognizant Key)or the key (Non-CognizantKey) for data non-analyzing recording methodsThe title key (Title Key)without using Master key (Master Key) and disk ID (Disc ID)A key equivalent to a title inherent key (TitleUnique Key) may be generated from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key).

[0204]For examplewhen one of the transmission formats specified to above 5CDTCP is useddata may be transmitted by the TS packet of MPEG 2. For examplewhen the set top box (STB:Set Top Box) which received satellite broadcasting uses 5CDTCP for a record machine and transmits this broadcast to itIt does not have the necessity for data conversion that an IEEE1394 top also transmits the MPEG 2 TS packet transmitted with the satellite broadcasting channeland STB's is desirable.

[0205]The recording and reproducing device 1600 receives the contents data which should be recorded in the form of this TS packetand adds ATS which is the time information which received each TS packet in TS processing means 300 mentioned above. As explained previouslythe block seed added to block data may consist of values which combined ATScopy control informationand the information of further others.

[0206]As X individual (for exampleX= 32) puts in order the TS packet which added ATS1-block block data is formed (refer to the figure on drawing 5) and it is shown in drawing 16 and the lower berth of 17The block seed (Block Seed) who the 1-4th byte of the head of the block data inputted as encrypted data is separated (selector 1608)and contains ATS which is 32 bits by which ****** is carried outFrom the title inherent key (Title Unique Key) generated previouslyblock key (Block Key) which is a key which enciphers the data of the block is carried out generation 1607.

[0207]The example of the generation method of block key (Block Key) is shown in

drawing 23. By drawing 23each shows two examples which generate the 64-bit block key (Block Key) from 32 bits block seed (Block Seed) and a 64-bit title inherent key (Title Unique Key).
[0208]64 bits of key length and the code function whose input and output are 64 bitsrespectively are being used for Example 1 shown in the upper row. A title inherent key (Title Unique Key) is used as the key of this code functionand the result which inputted the value which connected the constant (constant) of 32 bits with block seed (Block Seed)and was enciphered is made into the block key (Block Key).
[0209]Example 2 is an example which used hash function SHA-of FIPS 180-1 1. The value which connected the block seed (Block Seed) with the title inherent key (Title Unique Key) is inputted into SHA-1What was contracted to 64 bitssuch as 64 bits of low ranks accepting the output of 160 bitsand using itfor exampleis made into the block key (Block Key).
[0210]Although the example which generates a disk inherent key (Disc Unique key)a title inherent key (Title Unique Key)and the block key (Block Key) aboverespectively was explainedFor examplewithout performing generation of a disk inherent key (Disc Unique Key) and a title inherent key (Title Unique Key)It is with master key (Master Key) for every block. Stamper ID (Stamper ID)disk ID (Disc ID)title key (Title Key)and block seed (Block Seed)The key for data analysis recording methods (Cognizant Key) (in the case of Cognizant Mode)or the key for data non-analyzing recording methods (Non-Cognizant Key) (in the case of data a non-analyzing recording method (Non-Cognizant Mode)). It may use and the block key (Block Key) may be generated.
[0211]Generation of a block key will encipher block data using the generated block key (Block Key). As shown in drawing 16 and the lower berth of 17it dissociates (selector 1608)and the 1st - m byte (for examplem= 8) of the head of block data including the block seed (Block Seed) do not consider it as the candidate for encryptionbut does from the m+1st byte to final data encryption 1609. In m byte who is not encipheredthe 1-4th byte as BURROKU seed is also contained. The block data after the m+1st byte separated by the selector 1608 is made into the cipher-processing means 150 encryption 1609 according to the encryption algorithrn set up beforehand. As an encryption algorithmDES (Data Encryption Standard) specifiedfor example by FIPS 46-2 can be used.
[0212]As mentioned abovefor block seed. It is possible to include copy limit information (CCI:CopyControl Information)When recording processing in a data analysis recording method (Cognizant Mode) is performedThe copy control information corresponding to the embedding CCI (Embedded CCI) which is the copy control information (CCI) embedded to the inside of contents data is recordedWhen recording processing in data a non-analyzing recording method (Non-CognizantMode) is performedthe copy control information reflecting EMI (Encyrption Mode Indicator) on the packet header explained by drawing 20 is recorded.
[0213]In namelythe case of the Information Storage Division processing by a data

analysis recording method (Cognizant Mode). The block seed including the copy control information based on the embedding copy control information (CCI) in a data divisionRecorded information generation processing added to the block data which consists of one or more packets is performedIn the case of the Information Storage Division processing by data a non-analyzing recording method (Non-Cognizant Mode). Recorded information generation processing which added the block seed including the copy control information based on the encryption mode indicator (EMI) as copy control information included in a packet to the block data which consists of one or more packets is performed.

[0214]Herewhen the block length (input-and-output data size) of the cryptographic algorithm to be used is 8 bytes like DESX is set to 32it is making m into the multiple of 8and the whole block data after the m+1st byte can be enciphered without a fraction.

[0215]That iswhen the number of the TS packet stored in 1 block is made into X individualinput-and-output data size of a cryptographic algorithm is made into L byte and n is made into arbitrary natural numbersa fraction process becomes unnecessary by setting Xmand L that 192*X=m+n*L is realized.

[0216]With the 1st - m byte data in which cipher processing is not carried outit is combined by the selector 1610 and the block data after the m+1st enciphered byte is stored in the recording medium 1620 as the enciphered content 1612.

[0217]Contents are block unitsand encryption is given by the above processing with the block key generated based on the master key by which generation management was carried outthe block seed containing ATSetc.and they are stored in a recording medium by it.

[0218]As mentioned abovesince contents data is enciphered in this composition with the master key by which generation management was carried out and it is stored in the recording mediumIt becomes decodingi.e.the conditions which become refreshablethat it is a record reproducer which has a generation newer than the generation of the master key used when regeneration [in / for the recording medium / other record reproducers] recorded the same generation or data at least.

[0219]A block key as mentioned above in record of a data analysis recording method (Cognizant Mode)It is generated based on the key for data analysis recording methods (Cognizant Key)andin data non-analyzing recording method (Non-Cognizant Mode) recordis generated based on the key for data non-analyzing recording methods (Non-Cognizant Key). These encryption data becomes refreshable only by apparatus with the key (the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key)) corresponding to the same mode as the time of record.

[0220]Namelythe key for data analysis recording methods (Cognizant Key)Only the apparatus allowed reproduction of apparatus with the capability which recognizes Embedded CCI embedded into the stream at the time of recordand is updated if neededand its data is givenBy apparatus without this keyreproduction of the

contents recorded by the data analysis recording method (Cognizant Mode) cannot be performed.
[0221]Similarly the key for data non-analyzing recording methods (Non-Cognizant Key)Apparatus with the function of the recording mode of data a non-analyzing recording method (Non-Cognizant) which does not recognize the embedding CCI (Embedded CCI) in a stream at the time of recordOnly the apparatus allowed reproduction of the data recorded in that mode is givenand reproduction of the contents recorded by the data non-analyzing recording method (Non-Cognizant Mode) cannot be performed by apparatus without this key. The details of regeneration are mentioned later.
[0222]Nextaccording to the flow chart shown in drawing 18the flow of ATS attached processing in TS processing means 300 performed with the Data Recording Sub-Division processing and the whole processing of cipher processing in the cipher-processing means 150 is explained collectively. In S1801 of drawing 18The master key and the key for data analysis recording methods (Cognizant Key) (in the case of a data analysis recording method (CognizantMode))or the key for data non-analyzing recording methods which stores the recording and reproducing device in the own memory 180. (Non-CognizantKey) It reads (in the case of data a non-analyzing recording method (Non-Cognizant Mode)). Stamper ID (Stamper ID) is read from a disk.
[0223]In S1802it is inspected whether disk ID (Disc ID) as identification information is already recorded on the recording medium. If are recordedand this disk ID is read and it is not recorded by S1803by S1804disk ID is generated by the method defined at random or beforehandand it records on a disk. Nextat S1805it is a master key. A disk inherent key is generated using stamper ID (Stamper ID) and disk ID. It asks to have explained the disk inherent key previously by applying the method of using hash function SHA-1 defined by FIPS 180-1the method of using the hash function based on a block cipheretc.
[0224]Nextit progresses to S1806the title key (Title Key) as a peculiar key for the one reccrd of every is generatedand it records on a disk with the generation number of a recording mode (Recording Mode) and a master key. A recording mode (Recording Mode) shows whether the Information Storage Division mode to perform is a data analysis recording method (Cognizant Mode) or it is data a non-analyzing recording method (Non-CognizantMode).
[0225]By S1807nextan above-mentioned disk inherent key and title keyThe key for data analysis recording methods (Cognizant.) A title inherent key is generated from Key (in the case of a data analysis recording method (Cognizant Mode))or the key for data non-analyzing recording methods (Non-Cognizant Key) (in the case of data a non-analyzing recording method (Non-Cognizant Mode)).
[0226]The detailed flow of generation of a title inherent key is shown in drawing 24. The cipher-processing means 150 branches by a recording mode in Step S2001. This branching is judged based on the indicative data inputted by the user who a record reproducer programs or uses a record reproducer.
[0227]When a recording mode is a data analysis recording method (Cognizant

Mode)i.e.Cognizant recordin S2001It progresses to Step S2002 and a title inherent key (Title Unique Key) is generated from a disk inherent key (Disc UniqueKey)title key (Title Key)and the key for data analysis recording methods (Cognizant Key).
[0228]When a recording mode is data a non-analyzing recording method (Non-Cognizart Mode)i.e.Non-Cognizant recordin S2001Progress to Step S2003 and A disk inherent key (Disc Unique Key) and the title key (Title Key)From the key for data non-analyzing recording methods (Non-Cognizant Key)a title inherent key (Title Unique Key) is generated. The hash function based on the method and block cipher which use SHA-1 is used for key generation.
[0229]A recording and reproducing device receives S1808 the encrypted data of the contents data which should be recorded in the form of a TS packet. By S1809TS processing means 300 adds ATS which is the time information which received each TS packet. Or the value which combined the copy control information CCI and ATS and the information of further others is added. Nextit is judged whether the TS packet which added ATS was received one by one by S18101 block is formedfor examplethe identification data in which whether it having amounted to X= 32 and the end of a packet are shown was received. When one of conditions is satisfiedit progresses to Step S1811and the packet to X individual or the end of a packet is put in orderand 1-block block data is formed.
[0230]Nextthe cipher-processing means 150 is S1812 and generates the block key which is a key which enciphers the data of the block from 32 bits (block seed containing ATS) of the head of block dataand the title inherent key generated by S1807.
[0231]In S1813the block data formed by S1811 using the block key is enciphered. As explained also in advanceit is the m+1st byte to final data of block data that it is the target of encryption. DES (Data Encryption Standard) as which an encryption algorithm is specifiedfor example by FIPS 46-2 is applied.
[0232]By S1814the enciphered block data is recorded on a recording medium. By S1815it is judged whether all the data was recorded. If all the data is recordedrecording processing is ended and all the data is not recordedit will return to S1808 and processing of the remaining data will be performed.
[0233]Recording processing of contents is performed by a data analysis recording method (Cognizant Mode)or data either a non-analyzing recording method (Non-Cognizant Mode) according to above-mentioned processing. When recording processing of contents is performed by a data analysis recording method (Cognizant Mode)The key applied to encryption of contents is generated based on the key for data analysis recording methods (Cognizant Key)When recording processing of contents is performed by data a non-analyzing recording method (Non-Cognizant Mode)the key applied to encryption of contents will be generated based on the key for data non-analyzing recording methods (Non-Cognizant Key). Therefore the contents recorded on the disk in each methodThe key for data analysis recording methods used at the time of record (Cognizant Key)Or it becomes indispensable to generate the key for decoding with the application of either of the keys for data non-analyzing recording methods (Non-Cognizant Key)

and the same keyand the record and regeneration in which the all directions type was intermingled are prevented.
[0234][The writing of confidential information and reproduction] Nextconfidential informationsuch as stamper ID shown in drawing 16drawing 17etc.Only when the technique of writing in a disk in a different mode from the usual data writing techniqueand being different from the usual data read is appliedthe writing and the example of reading processing composition of confidential information which were made into the mode which can be read are explained.
[0235](Confidential information generation by the turbulence of a signal) The composition which carries out the turbulence of the variety-of-information signalssuch as stamper IDwith an M sequence signaland records them is explained first.
[0236]The write signal generation modulation circuit composition for the writing processing of confidential information is shown in drawing 25. Whenever the disk original recording which is a data writing object rotates only a predetermined anglethe modulation circuit shown in drawing 25 modulates confidential informationsuch as La Stampa IDon the basis of the FG signal with which a signal level risesand performs writing.
[0237]PLL circuit 1041 generates channel clock CK which synchronized with rotation of disk original recording on the basis of the FG signaland supplies it to each part of a modulation circuit.
[0238]The timing generator 1042 generates the initialization pulses SY which initialize the M sequence generation circuits 1045A-1045D with a predetermined time interval by counting channel clock CK. The timing generator 1042 generates and outputs alignment pattern selection signal ST in sync with the initialization pulses SY.
[0239]in the modulation circuit shown in drawing 25it is markedly alike to channel clock CKand confidential informationsuch as stamper IDis inputted by the late bit rate. The alignment pattern generation circuit 1043 generates and outputs the predetermined alignment pattern DY on the basis of the standup of the initialization pulses SY.
[0240]The M sequence generation circuits 1045a-1045D are initialized by the initialization pulses SYand output M sequences M1-M4 which change per channel clock CK. A logical value changes at random and M sequences M1-M4 are data rows which are establishment [probability of occurrence / of the logic 1 and the logic 0] here.
It did not correlate mutually.

[0241]Arithmetic circuit (X)s 1046A-1046D are constituted by the exclusive OR circuitperform each bits b0-b3 and exclusive-or operations of confidential informationsuch as the M sequence signals M1-M4La Stampa IDdisk IDrespectivelyand output the result of an operation. Therebythe turbulence of the confidential informationsuch as stamper IDis carried out by the M sequence signals M1-M4.

[0242]The random number generation circuit 1047 generates the 2-bit random number (one value of 012and 3) R per channel clock CKand outputs it to the data selector 1048. The data selector 1048 carries out the selected output of the result of an operation of the arithmetic circuits 1046A-1046D according to the value of the random number R. For exampleit is considered as the output selection of the arithmetic circuit 1046D at the time of the output selection of the arithmetic circuit 1046Cand the random number R= 3 at the time of the output selection of the arithmetic circuit 1046Band the random number R= 2 at the time of output selection [of the arithmetic circuit 1046A]and random number R=1 at the time of the random number R= 0.
[0243]By this compositionthe modulation circuit is enabling composition which makes one line the result of an operation of 1046A-1046Dand carries out turbulence furtherwithout decoding on the basis of corresponding M sequences M1-M4 receiving the influence by other results of an operation.
[0244]The data selector 1049 carries out the selected output of the output of alignmert pattern DY outputted from the alignment pattern generation circuit 1043 on the basis of alignment pattern signal STand the data selector 1048. Therebyafter the initialization pulses SY risethe output of the data selector 1048 is performed after the alignment pattern between predetermined clock periodsfor example5 clock periods[ex.11011].
[0245]The output generated by the predetermined confidential information writing area in the modulation circuit shown in drawing 25 is written in disk original recording. Even when confidential informationsuch as stamper ID inputted into a modulation circuitis the samewrite data modes will differ according to a random number. Thereforethe writing of data with difficult analysis is attained in the usual reading processing.
[0246]Nextregeneration of the confidential information written in by the above-mentioned technique is explained using drawing 26. Drawing 26 is a figure showing the decode processing means composition which decodes confidential informationsuch as digital regenerative signal DX to stamper ID read in the disk. PLL circuit 1081 plays channel clock CK generated at the time of record on the basis of digital regenerative signal DX read in the diskand outputs it to each part.
[0247]The synchronization detecting circuit 1082 detects an alignment pattern by discernment of digital regenerative signal DX on the basis of channel clock CKand reproduces the initialization pulses SY at the time of record by a detection result. The M sequence generation circuits 1083A-1083D output M sequences M1-M4 generated [on the basis of this initialization-pulses SY and channel clock CK] at the time of recordrespectively.
[0248]Multiplication circuit (X)s 1084A-1084D carry out the multiplication of digital regenerative signal DX to the M sequence signals M1-M4respectivelyand output a multiplication result. Multiplication circuit (X)s 1084A-1084D perform this multiplication processing here by reversing the polarity of digital regenerative signal DX according to the logical value of the M sequence signals M1-M4. Digital regenerative signal DX is correctly reproduced by only decoding on the basis of

corresponding M sequences M1-M4.
[0249]The integration circuits 1085A-1085D output the integrated result of the value according to the logical value of the bit strings b1-b3 to which confidential informationsuch as stamper IDcorresponds by integrating with the multiplication result outputted by the multiplication circuits 1084A-1084D on the basis of the initialization pulses SYrespectively. The decision circuits 1086A-1086D decode and output each bits b0-b3 of confidential informationsuch as stamper IDby carrying out binary identification of the integrated result outputted from the integration circuits 1085A-1085Drespectively on the basis of the initialization pulses SY.
[0250]As mentioned aboveconfidential informationsuch as stamper IDis inputted into a modulation circuit (drawing 25) as 4 bit-parallel bit strings b0-b3and since four M sequences M1-M4 and the turbulence by the random number R are made and recordedit becomes difficult to read [reading processing / usual] it. The output of confidential informationsuch as stamper IDis attained by decoding of a reading signal by the M sequence which became generable and generated M sequences M1-M4 on the basis of the alignment pattern DY at the time of reproduction.
[0251]The recording and reproducing device which reads stamper ID written in by the above-mentioned recording methodand generates the cipher-processing key of contents based on stamper ID etc. has confidential information decode processing means composition with the composition of drawing 26.
[0252]Confidential information to (disk inner circumference as an example from which record) next the writing of confidential informationand regeneration differConfidential informationsuch as La Stampa IDis written in a different disk area from writing areassuch as music dataand the composition which made it possible to read this stably by a focus servo is explained.
[0253]Drawing 27 is a perspective view showing the disk which recorded confidential informationsuch as La Stampa ID. Repetition record is carried out 4 times at 1 round of a diskand confidential informationsuch as stamper IDis constituted so that playback of confidential information may be attainedeven when damage occurs selectively. Confidential information has information areassuch as a header and stamper IDand the composition to which the error correcting code was assigned further. each bit of the bit pattern which shows these information is markedly boiled as compared with each bit of the data area recorded as an user datumit is longfor examplethe very small field of a 50-micrometer unit is formed as a unit. The alignment pattern in which the pattern to which the optical property of the recording surface was changed was formed is formed in the information area of stamper IDand an error correcting code fieldand the timing control at the time of reproduction only of the central region of three very small fields becomes possible with this alignment pattern to them.
[0254]Information areassuch as stamper IDand error correcting code area informationData is divided every 2 bitswhen 2 bit data (b1b0) are the logic 00as shown in drawing 27 (D1)change is generatedand the optical property of the

recording surface of only a top very small field is changed and recorded on logic [1000]. Hereafterit is referred to as [0001]when 2 (D2) bit data (b1b0) are the logic 01[0100] and 2 (D3) bit data (b1b0) are the logic 10 and [0010] and 2 (D4) bit data (b1b0) are the logic 11. Therebyon a diskit becomes 0.3 or lessand also in a disk inner circumference fieldthe rate of an abundance ratio of the field where the optical property changed makes possible the focus servo by sufficient reflected light quantityand becomes possible about data reading.

[0255]Drawing 28 is a figure showing the decode processing means composition used for reading of confidential informationsuch as stamper ID recorded on the disk inner circumference field. PLL circuit 1160 carries out the reproducing output of channel clock CK from digital regenerative signal DX.

[0256]By judging the signal level of digital regenerative signal DX on the basis of channel clock CKthe synchronization detecting circuit 1161 detects an alignment patternand outputs the initialization pulses SY.

[0257]The timing generator 1162 outputs the sampling pulses T1-T4 of each very small field which rise in the center mostlyrespectively about the 1-4th very small fields shown in drawing 27 which follows an alignment pattern on the basis of the initialization pulses SY.

[0258]Flip-flop (FF) 1163A-1163D latch a digital regenerative signal on the basis of the sampling pulses T1-T4respectively. The signal level of the regenerative signal acquired by this from information areassuch as La Stampa ID and disk IDand four very small fields assigned to 2 bits each of error correcting code area information is latched to the flip-flops 1163A-1163Drespectivelyand is held.

[0259]The maximum detector circuit 1164 by these four latches' D1-D4 size judgment. Decodeoutput 2 bit data (b1b0) of information areassuch as stamper ID and disk IDand an error correcting code fieldand the parallel serial conversion circuit (PS) 1165One by one2 bit data (b1b0) outputted from the maximum detector circuit 1164 are changed into serial dataand are outputted.

[0260]The recording and reproducing device which reads stamper ID written in by the above-mentioned recording methodand generates the cipher-processing key of contents based on stamper ID etc. has confidential information decode processing means composition for the composition of drawing 28.

[0261]Thusthe composition of a different special confidential information write-in technique from contents and the technique to read is adoptedSince it had composition used as source data of the key which stores confidential informationsuch as stamper IDin a diskand applies this to encryption of contentsand decoding processingEven if other processing keys are revealedit will become confidential informationsuch as stamper ID stored in the diskis difficult to readand possible to make the possibility of disclosure decrease sharplyand the contents protection which raised security more will be attained.

[0262]Although the example which set up the confidential information of which the specific data writing processing stored in a disk and regeneration are required in this Description as stamper ID is explainedIt is possible to set up not only stamper ID but various identification datasuch as disk ID set up by differing for every

diskcontent ID differed and set up for every contentsor a key for cipher processingand a cipher-processing key as confidential information stored in a disk. The cipher-processing key of contents is generated with the application of such various confidential information.
[0263]As shown in drawing 16 and drawing 17the recording and reproducing device mentioned above The encryption for data analysis recording method (Cognizant Mode) recordThe key for decoding processing key generation (key for data analysis recording methods (Cognizant Key))Although it is usable composition selectivelythe encryption for data non-analyzing recording method (Non-Cognizant Mode) recordand both sides with the key for decoding processing key generation (key for data non-analyzing recording methods (Non-Cognizant Key))In the record reproduction apparatus which performs one of methodsonly one of keys (Cognizant Key)i.e.the key for data analysis recording methodsor the key for data non-analyzing recording methods (Non-Cognizant Key) is stored.
Based on a storing keyencryption of contents and the block key for decoding processings are generated.
The block diagram showing the generation processing process of the cipher-processing key of the contents in the recording and reproducing device which stored these independent keys is shown in drawing 29 and drawing 30.
[0264]Drawing 29 is a recording and reproducing device which has only a key for data analysis recording methods (Cognizant Key).
It is the composition of generating the cryptographic key and decryption key which are used in the case of the data reproduction from Data Recording Sub-Division and the recording medium to a recording medium based on key generation data besides the key for data analysis recording methods (Cognizant Key)and performing encryption of contentsand decoding.

[0265]Drawing 30 is a recording and reproducing device which has only a key for data non-analyzing recording methods (Non-Cognizant Key).
It is the composition of generating the cryptographic key and decryption key which are used in the case of the data reproduction from Data Recording Sub-Division and the recording medium to a recording medium based on key generation data besides the key for data non-analyzing recording methods (Non-Cognizant Key)and performing encryption of contentsand decoding.

[0266]In such independent key enclosureexecution of record of data and reproduction is attained only in one of methods.
[0267][Contents data decryption with the master key in which generation management was made and regeneration] Nextthe processing which decodes the enciphered content recorded on the recording medium as mentioned aboveand is reproduced is explained to be a processing block figure of drawing 31 using the flow chart of drawing 32 - drawing 34.
[0268]According to the flow chart shown in drawing 32the flow of processing is explained about decoding processing and regenerationreferring to the processing

block figure of drawing 31. In S2401 of drawing 32the recording and reproducing device 2300 (refer to drawing 31) reads disk ID2302pre (pre-recording) record generation numberand stamper ID(Stamper ID) 2380 from the disk 2320The master key 2301the key 2331 for data analysis recording methods (Cognizant Key) and/or the key 2332 for data non-analyzing recording methods (Non-Cognizant Key) is read from an own memory. It is the identifier peculiar to a disk which disk ID was beforehand recorded on the diskor was generated in the record reproducer and recorded on the disk when that was not right so that clearly from explanation of previous recording processing.

[0269]The pre (pre-recording) record generation number 2360 is the generation information peculiar to a disk stored in the disk which is a recording medium beforehand. This pre (pre-recording) generation number is compared with the generation number 2350 of the master key at the time of Data Recording Sub-Divisioni.e.a record times cost numberand the propriety of regeneration is controlled. The master key 2301 is the secret key by which it was stored in the memory of a recording and reproducing device by the flow of drawing 14and generation management was made. The key for data analysis recording methods (Cognizant Key)and the key for data non-analyzing recording methods (Non-Cognizant Key)It is a secret key common to a system corresponding to a data analysis (Cognizant) recording modeand data the recording mode non-analyzing (Non-Cognizant)respectively.

[0270]Nextthe recording and reproducing device 2300 is S2402and reads the generation number (Generation #) 2350 of the title key of the data which should be read from a diskand the master key further used when the recording mode of data and data were recordedi.e.a record times cost number. Nextit is judged whether the data which should be read by S2403 is refreshable. The detailed flow of a judgment is shown in drawing 33.

[0271]In Step S2501 of drawing 33a recording and reproducing device judges old and new [of the pre generation number read by S2401and the record times cost number read by S2402]. When judged with the generation whom a record times cost number shows not being after the generation whom pre record generation information expressesThat iswhen the generation whom the Data Recording Sub-Division times cost information expresses is a generation older than the generation whom pre record generation information expressesit judges that reproduction is impossibleSteps S2404 thru/or S2409 are skippedand processing is endedwithout regenerating. Thereforewhen the contents recorded on the recording medium are enciphered based on the master key of a generation older than the generation whom pre record generation information expressesthe reproduction is not permitted and reproduction is not performed.

[0272]Namelythis processing is an inaccurate recorder with which injustice will be revealed and the newest generation's master key will not be givenIt is the processing to which it was presupposed that reproduction of the recording medium on which data was encipheredit was judged as the thing applicable when recorded on a recording medium based on an old generation's master keyand data was

recorded by such an inaccurate device is not performed. Therebyuse of an inaccurate recorder can be eliminated.

[0273]On the other hand in Step S2501the generation whom a record times cost number expressesWhen judged with it being after the generation whom a pre record generation number expressesthe generation whom record times cost information expressesThey are whether to be the same as that of the generation n whom a pre record generation number expressesand a new generationThereforewhen the contents recorded on the recording medium are enciphered based on the master key of the generation after the generation whom pre record generation information expresses. Progressing to Step S2502a recording and reproducing device acquires the generation information of the encryption master key C which the own memory has memorizedcompares the generation of the encryption master key with the generation whom code times cost information expressesand judges the generation order.

[0274]In Step S2502the generation of the master key C memorized by the memoryWhen judged with it not being after the generation whom record times cost information expressesthe generation of the master key C memorized by the memoryWhen it is a generation older than the generation whom record times cost information expressesit judges that reproduction is impossibleSteps S2404 thru/or S2409 are skippedand processing is endedwithout regenerating.

[0275]On the other hand in Step S2502the generation of the encryption master key C memorized by the memoryWhen judged with it being after the generation whom record times cost information expressesthe generation of the master key C memorized by the memoryThe same as that of the generation whom record times cost information expresses or Or when newer than itIt progresses to Step S2503 and it is judged whether playback apparatus itself owns the key corresponding to the mode at the time of recordi.e.the key for data analysis recording methods(Cognizant Key)and the key for data non-analyzing recording methods (Non-Cognizant Key).

[0276]In Step S2503when playback apparatus itself owns the key for data analysis recording methods (Cognizant Key) or the key for data non-analyzing recording methods (Non-Cognizant Key) which is a key corresponding to the mode at the time of recordit judges that it is refreshable. When playback apparatus itself does not own the key (the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key)) corresponding to the mode at the time of recordit judges with reproduction being impossible.

[0277]When judged with it being refreshableit progresses to Step S2404. In S2404a disk inherent key (Disc Unique Key) is made disk ID (Disc ID) and master key (Master Key) generation 2302 using stamper ID (Stamper ID). This key generation method to hash function SHA-1 defined by FIPS 180-1for example. The data generated by the bit connection to a master key and disk ID (Disc ID) is inputtedThe method of using only required data length as a disk inherent key (Disc Unique Key) from the output of 160 bitsMethodssuch as using the result obtained

by inputting master key (Master Key) and disk ID (Disc ID) into the hash function using a block cipher functionare mentioned. The master key used here is a master key of the generation (at the time) whom the record times cost number of the data read from the recording medium expresses with Step S2402 of drawing 32. When the master key of the generation in which a recording and reproducing device is newer than this is heldthe master key of the generation whom a record times cost number expresses using the method mentioned above may be createdand a disk inherent key (Disc Unique Key) may be generated using it.

[0278]Nexta title inherent key is generated by S2405. The detailed flow of generation of a title inherent key is shown in drawing 34. The cipher-processing means 150 performs the judgment of a recording mode in Step S2601. This judgment is performed based on the recording mode (Recording Mode) read from the disk.

[0279]When judged with a recording mode being a data analysis recording method (Cognizant Mode) in S2601It progresses to Step S2602 and a title inherent key (Title Urique Key) is generated from a disk inherent key (DiscUnique Key)title key (Title Key)and the key for data analysis recording methods (Cognizant Key).

[0280]When judged with a recording mode being data a non-analyzing recording method (Non-CognizantMode) in S2601Progress to Step S2603 and A disk inherent key (Disc Unique Key) and the title key (Title Key)From the key for data non-analyzing recording methods (Non-Cognizant Key)a title inherent key (Title Unique Key) is generated. The hash function based on the method and block cipher which use SHA-1 is used for key generation.

[0281]By the above-mentioned explanationit is with master key (Master Key). A disk inherent key (Disc Unique Key) is generated from stamper ID (Stamper ID) and disk ID (Disc ID)This and title key (Title Key) A title inherent key (Title Unique Key) from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key). Although he is trying to generaterespectivelyIt is with master key (Master Key)using a disk inherent key (Disc Unique Key) as unnecessary. Stamper ID (Stamper ID)disk ID (Disc ID)and the title key (Title Key)a title inherent key (Title Unique Key) being directly generated from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key)andWithout using the title key (Title Key)Master key (Master Key)stamper ID (Stamper ID)and disk ID (DiscID)A key equivalent to a title inherent key (Title Unique Key) may be generated from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key).

[0282]Nextread the block data (Block Data) from the enciphered content 2312 enciphered and stored from the disk by S2406 one by oneand by S2407. 4 bytes of block seed (Block Seed) of the head of block data is separated in the selector 2310and a block key is generated using block seed (Block Seed) and the title inherent key generated by S2405.

[0283]The generation method of block key (Block Key) can apply the composition

of drawing 23 explained previously. That isthe composition which generates the 64-bit block key (Block Key) is applicable from 32 bits block seed (Block Seed) and a 64-bit title inherent key (Title Unique Key).
[0284]Although the above-mentioned explanation explained the example which generates a disk inherent key (Disc Unique key)a title inherent key (Title Unique Key)and the block key (Block Key)respectivelyFor examplewithout performing generation of a disk inherent key (Disc Unique Key) and a title inherent key (Title Unique Key)It is with master key (Master Key) for every block. Stamper ID (Stamper ID)disk ID (Disc ID)and the title key (Title Key)The block key (Block Key) may be generated using block seed (Block Seed)and the key for data analysis recording methods (Cognizant Key) or the key for data non-analyzing recording methods (Non-Cognizant Key).
[0285]If a block key is generatednextby S2408the block data enciphered using the block key (Block Key) will be carried out decoding 2309and it will output as decode data via the selector 2308. ATS is added to each transport packet which constitutes a transport stream in decode data.
Stream processing based on ATS is performed in TS processing means 300 explained previously.
Thendata becomes possible [using it displaying a pictureor playing music].
[0286]Thusdecoding processing is performed with the block key generated based on the block seed containing ATS by a block unitand reproduction of the enciphered content which was enciphered by the block unit and stored in the recording medium is attained. The block data enciphered using the block key is decodedif it judged whether all the data was read and all the data is read by S2409it will endotherwiseit returns to S2406and the remaining data is read.
[0287]As shown in drawing 31the recording and reproducing device mentioned above The encryption for data analysis recording method (Cognizant Mode) record and the key for decoding processing key generation (key for data analysis recording methods (Cognizant Key))Although it is an usable example of composition selectivelythe encryption for data non-analyzing recording method (Non-Cognizant Mode) recordand both sides with the key for decoding processing key generation (key for data non-analyzing recording methods (Non-Cognizant Key))As previously explained to drawing 29 and drawing 30it is shown and One of keysNamelythe key for data analysis recording methods (Cognizant Key)Or in the apparatus which stored only the key for data non-analyzing recording methods (Non-Cognizant Key)only the method corresponding to one of storing keys is performedand the block key for the decoding processings of contents is generated based on a storing key.
[0288]In above-mentioned working example in timewith [the processing constitution which uses a medium key effective only in a recording medium]The master key was transmitted to each recording and reproducing device using validation key blocks (EKB:EnablingKey Block)and it was supposed that a recording and reproducing device performs record of dataand reproduction using this.
[0289]A master key is a key effective in the whole record of the data at the time.

It enables the recording and reproducing device which was able to obtain the master key at a certain time to decode the data recorded by this system before it at that t me.
Howeverthere is also fault that the influence of [at the time of being exposed of a master key to an aggressor] attains to the whole system on the character of an effective flume lie by the whole system.
[0290]On the other handit becomes possible to suppress the influence of disclosure of a key by using as a medium key effective only in the recording medium instead of a master key effective in all the systems the key transmitted using EKB (Enabling Key Block) of a recording medium. The method which uses a medium key for below instead of a master key as the 2nd working example is explained. Howeveronly a changed part with the 1st working example is explained.
[0291]Updating node key K(t)00 are generated using the leaf key K0000 and the node key K000 which EKB and the them at the t time by which the device 0 is stored in the recording medium store in drawing 35 beforehand as the same example as drawing 13and K00Signs that updating medium key:K(t) media is obtained using it are shown. K(t) media obtained here is used at the time of record of the data of the recording mediumand reproduction.
[0292]Since there is no concept of old and new [of a generation] like a master key in a medium keythe pre record generation number (Generation #n) in drawing 35 is set up as an option rather than is indispensable.
[0293]When a recording medium is inserted in a recording and reproducing device for record of dataor reproductionwith the flow chart shown in drawing 36each recording and reproducing device calculates medium key:K(t) media for the recording mediaand uses it for access to the recording medium behindfor example.
[0294]Reading of EKB of Step S2801 of drawing 36 and processing of EKB of S2802 are the respectively same processings as Steps S1403 and S1404 of drawing 14.
[0295]In Step S2803a recording and reproducing device reads the cryptogram Enc (K(t) 00 and K (t) media) which enciphered medium key K(t) media by node key K(t)00 from a recording mediumdecodes this at Step S2804and obtains a medium key. If RIBOKU [this recording and reproducing device / group / who shows drawing 11 / of tree composition / eliminate namely]a medium key cannot be obtained and record to that recording medium and reproduction cannot be performed.
[0296]Nextalthough processing of record of the data to a recording medium is explainedSince there is no concept of old and new [of a generation] like a master key in a medium keyThe check of whether record by comparison of the generation of the master key which pre record generation information and the recording and reproducing device itself store who showed drawing 15 the 1st working example is possible is not performedbut it is judged that it is recordable if the medium key has been obtained in the above-mentioned processing. That isit becomes like the process flow shown in drawing 37. The process flow of drawing 37 judges acquisition of a medium key by S2901and only when acquiredit performs recording

processing of contents in Step S2902.
[0297][Recording processing of the data which uses a medium key effective only in a recording medium] The situation of the recording processing of contents data is explained using drawing 38the block diagram of 39and the flow chart of drawing 40.
[0298]Let an optical disc be an example as a recording medium like the 1st working example in this example. In order to prevent bit-by-bit copy of the data on a recording medium in this working examplethe point of trying to make disk ID (Disc ID) as identification information peculiar to a recording medium acting on the key which enciphers data is also the same.
[0299]Drawing 38 and drawing 39 are the figures corresponding to the 1st drawing 16 and drawing 17 in working examplerespectively.
It differs in that the record times cost number (Generation #) which it differs in that the medium key (Media Key) is used instead of master key (Master Key)and shows the generation of a master key is not used.
The difference between drawing 38 and drawing 39 is a difference [performing the writing of disk ID like the difference between drawing 16 and drawing 17] which lends and is not.
[0300]Drawing 40 shows the Data Recording Sub-Division processing in this example which uses a medium keyand corresponds to the flow chart of drawing 18 (working example 1) mentioned above. Hereaftera point which is different from working example 1 about the process flow of drawing 40 is explained as a center.
[0301]The recording and reproducing device 3000 is stored in an own memory in S3201 of drawing 40. The key for data analysis recording methods (Cognizant Key) and/or the key for data non-analyzing recording methods (Non-Cognizant Key)It calculates by S2804 of drawing 36and medium key K(t) media saved temporarily is read. Stamper ID (Stamper ID) is read from a disk.
[0302]In S3202a recording and reproducing device inspects whether disk ID (Disc ID) as identification information is already recorded on the recording medium (optical disc) 3020. If are recordedand this disk ID (Disc ID) is read (equivalent to drawing 38) and it is not recorded by S3203by S3204disk ID (Disc ID) is generated by the method defined at random or beforehandand it records on a disk (equivalent to drawing 39). The thing with one stored in read in area etc. since it is good is also possible for disk ID (Disc ID) on the disk. In any caseit progresses to S3205 next.
[0303]Medium key read in S3205 S3201 A disk inherent key (Disc Unique Key) is generated using stamper ID (Stamper ID) and disk ID (Disc ID). It is the same method as the method used in the 1st working exampleand what is necessary is just to use a medium key instead of a master key as a concrete generation method of a disk inherent key (Disc Unique Key).
[0304]next -- progressing to S3206 -- the one record of every -- the peculiar key:title key (Title Key) -- random -- or eye dirt ** -- it generates by the **** methodlawsand records on a disk. Simultaneouslya recording mode (Recording Mode) when this title (data) is recorded is recorded on a disk.

[0305]On a diskthe data management file in which the information what data constituted what kind of title was stored isand a title key and RecordingMode can be stored in this file.
[0306]Since Steps S3207 thru/or S3215 are the same as that of S1807 thru/or S1815 of drawing 18explanation is omitted.
[0307]In the above-mentioned explanationa disk inherent key (Disc Unique Key) is generated from medium key (Media Key)stamper ID (Stamper ID)and disk ID (Disc ID)This and title key (Title Key) A title inherent key (Title Unique Key) from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key). Although he is trying to generaterespectivelyUsing a disk inherent key (Disc Unique Key) as unnecessary Medium key (Media Key)stamper ID (Stamper ID)disk ID (Disc ID)and the title key (TitleKey)a title inherent key (Title Unique Key) being directly generated from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key)andWithout using the title key (Title Key)Medium key (Media Key) Stamper ID (Stamper ID) and disk ID (Disc ID)A key equivalent to a title inherent key (Title Unique Key) may be generated from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key).
[0308]Data is recordable on a recording medium using a medium key as mentioned above.
[0309][Regeneration of the data which uses a medium key effective only in a recording medium] Nextthe situation of the processing which reproduces the data recorded as mentioned above is explained using the block diagram of drawing 41and the flow chart of drawing 42.
[0310]Drawing 41 is a figure corresponding to drawing 31 in the 1st working example.
It differs in that the medium key (Media Key) is used for a change of master key (Master Key)therefore the record times cost number (Generation #) is omitted.

[0311]In S3401 of drawing 42the recording and reproducing device 3400 stamper ID (Stamper ID) and disk ID (Disc ID) from the disk 3420 which is a recording mediumThe key for data analysis recording methods (Cognizant Key) and/or the key for data non-analyzing recording methods (Non-Cognizant Key)and the medium key that is calculated by S2804 of drawing 36 and saved temporarily are read from an own memory.
[0312]When drawing 36 is processed and a medium key is not able to be obtained at the time of insertion of this recording mediumit ends without regenerating.
[0313]Nextrecording-mode Recording Mode at the time of recording the title key (TitleKey) of the data which should be read from a diskand this data by S3402 is read.
[0314]Nextby S3403it is judged whether this data is refreshable. The details of processing of S3403 are shown in drawing 43.
[0315]At Step S3501it is judged whether the medium key (Media Key) was able to

be obtained. When a medium key is not able to be obtainedit becomes unreproducibleand when a medium key is able to be obtainedit progresses to Step S3502. The key corresponding to the recording mode which that of processing of Step S3502 is the same as that of S2503 of drawing 33and was used at the time of record of the data (in the case of a data analysis recording method (Cognizant Mode)) In the case of the key for data analysis recording methods (Cognizant Key)and data a non-analyzing recording method (Non-Cognizant Mode). When playback apparatus has a key for data non-analyzing recording methods (Non-Cognizant Key)judge "it is refreshable" and progress to Step S3404and in being otherit judges "reproduction is impossible"Steps S3404 thru/or S3409 are skippedand processing is endedwithout regenerating.

[0316]Since processing of Steps S3404 thru/or S3409 is the same as that of S2404 thru/or S2409 of drawing 32explanation is omitted.

[0317]By the above-mentioned explanationit is with medium key (Media Key). A disk inherent key (Disc Unique Key) is generated from stamper ID (Stamper ID) and disk ID (Disc ID)This and the title key (Title Key)Although he is trying to generate a title inherent key (Title Unique Key)respectively from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key)Using a disk inherent key (Disc Unique Key) as unnecessary Medium key (Media Key)stamper ID (Stamper ID)disk ID (Disc ID)and the title key (Title Key)A title inherent key (Title UniqueKey) may be directly generated from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key)Without using the title key (Title Key)Medium key (Media Key) Stamper ID (Stamper ID) and disk ID (Disc ID)A key equivalent to a title inherent key (Title Unique Key) may be generated from the key for data analysis recording methods (Cognizant Key)or the key for data non-analyzing recording methods (Non-Cognizant Key).

[0318]Record of the data to a recording medium and regeneration from a recording medium are performed as mentioned above.

[0319][Copy control in recording processing Nowin order to protect profitssuch as an owner of a copyright of contentsin the licensed deviceit is necessary to control the copy of contents.]

[0320]That isto record contents on a recording mediumthe contents investigate whether t is what may be copied (a copy is possible)and it is necessary to make it record only the contents which may be copied. When reproducing and outputting the contents recorded on the recording mediumthe illegal copy of the contents to output needs to be made not to be carried out later.

[0321]Thenprocessing of drawing 1 in the case of performing record reproduction of contents or the recording and reproducing device of drawing 2 is explained with reference to the flow chart of drawing 44 and drawing 45performing copy control of such contents.

[0322]Firstwhen recording the contents of the digital signal from the outside on a recording mediumrecording processing according to the flow chart of drawing 44

(A) is performed. Processing of drawing 44 (A) is explained. The record reproducer 100 of drawing 1 is explained as an example. If the contents (digital contents) of a digital signal are supplied to input-and-output I/F120 via an IEEE1394 serial bus etc.in Step S4001input-and-output I/F120 will receive the digital contentsand they will follow it to Step S4002for example.

[0323]In Step S4002it is judged whether the digital contents which received can copy input-and-output I/F120. That isthe contents are judged [that it can copy and] when the contents which input-and-output I/F120 received are not enciphered for example (for examplewhen the contents of a plaintext are supplied to input-and-output I/F120without using above-mentioned DTCP).

[0324]It shall suppose that the recording and reproducing device 100 is a device based on DTCPand processing shall be performed according to DTCP. 2-bit EMI (Encryption Mode Indicator) as copy control information for controlling a copy is prescribed by DTCP. When EMI is 00B (B expresses that the value before that is a binary number)Contents express that it is copy-free (Copy-freely)and when EMI is 01Bcontents express that it is what (No-more-copies) cannot carry out the copy beyond it. It expresses that contents are what (Copy-one-generation) may be copied only once when EMI is 10Band when EMI is 11Bcontents express that it is what (Copy-never) the copy is forbidden.

[0325]EMI is contained in the signal supplied to input-and-output I/F120 of the recording and reproducing device 100and contents are judged [that it can copy and] when the EMI is Copy-freely and Copy-one-generation. Contents are judged [that it cannot copy and] when EMI is No-more-copies and Copy-never.

[0326]In Step S4002when judged [that contents cannot be copied and]Steps S4003-S4005 are skippedand recording processing is ended. Thereforecontents are not recorded on the recording medium 10 in this case.

[0327]In Step S4002when judged [that contents can be copied and]it progresses to Step S4003 and processing in Step S302 of drawing 3 (A)S303and S304 and same processing are hereafter performed in Steps S4003-S4005. That isATS addition to the transport packet by TS processing means 300 and encryption processing in the cipher-processing means 150 are performedthe enciphered content obtained as a result is recorded on the recording medium 195and recording processing is ended.

[0328]EMI is contained in the digital signal supplied to input-and-output I/F120. When digital contents are recordedthe informationincluding for exampleembedded CCI in DTCPetc.which expresses a copy control state like EMI or EMI with the digital contents is also recorded.

[0329]Under the present circumstancesgenerallythe information showing Copy-One-Generation is changed and recorded on No-more-copies so that the copy beyond it may not be allowed.

[0330]In the recording and reproducing device of this inventioncopy control informationsuch as this EMIembedded CCIetc.is recorded in the form added to a TS packet. That islike Example 2 of drawing 10or Example 332 bits which added 24

bits thru/or 30 bitsand copy control information for ATS are added to each TS packetas shown in drawing 5.
[0331]When recording the contents of the analog signal from the outside on a recording mediumrecording processing according to the flow chart of drawing 44 (B) is performed. Processing of drawing 44 (B) is explained. When the contents (analog content) of an analog signal are supplied to input-and-output I/F140input-and-output I/F140In Step S4011the analog content which received the analog contentand progressed and received to Step S4012 judges whether it can copy or not.
[0332]Here the decision processing of Step S4012 to the signal received by input-and-output I/F140for example. It is carried out based on whether a macro vision (Macrovision) signal and a CGMS-A (Copy GenerationManagement System-Analog) signal are included. That iswhen a macro vision signal is recorded on the video cassette tape of a VHS methodit is a signal which serves as a noise. Analog content is judged [that it cannot copy and] when this is contained in the signal received by input-and-output I/F140.

[0333]For examplea CGMS-A signal is a signal which applied the CGMS signal used for the copy control of a digital signal to the copy control of the analog signalIt is expressed any of what (Copy-freely) has a free copy of contentsthe thing (Copy-one-generation) which may be copied only onceor the things (Copy-never) to which the copy is forbidden they are.
[0334]Thereforeanalog content is judged [that it can copy and]when a CGMS-A signal is included in the signal received by input-and-output I/F140 and the CGMS-A signal expresses Copy-freely and Copy-one-generation. Analog content is judged [that it cannot copy and] when the CGMS-A signal expresses Copy-never.
[0335]Analog content is judged [that it can copy and] when a macro vision signal and CGMS-A signal is not included in the signal received by input-and-output I/F4 for exampleeither.
[0336]In Step S4012when judged [that analog content cannot be copied and]Steps S4013 thru/or S4017 are skippedand recording processing is ended. Thereforecontents are not recorded on the recording medium 10 in this case.
[0337]In [when judged / that analog content can be copied and / progress to Step S4013 in Step S4012and] the following and Steps S4013 thru/or S4017Processing in Steps S322 thru/or S326 of drawing 3 (B) and same processing are performedand therebydigital conversionMPEG codingTS processingand encryption processing are madeand contents are recorded on a recording mediumand end recording processing.
[0338]When the CGMS-A signal is included in the analog signal received by input-and-output I/F140 and analog content is recorded on a recording mediumthe CGMS-A signal is also recorded on a recording medium. That isthis signal is recorded on the portion of the information on CCI shown by drawing 10or others. Under the present circumstancesgenerallythe information showing Copy-One-

Generation is changed and recorded on No-more-copies so that the copy beyond it may not be allowed. Howeverit is not this limitation when a rulesuch as "treating the copy control information of Copy-one-generation as No-more-copies although recorded without changing into No-more-copies"is decided in the system.
[0339][Copy control in regeneration] Nextwhen reproducing the contents recorded on the recording medium and outputting outside as digital contentsregeneration according to the flow chart of drawing 45 (A) is performed. Processing of drawing 45 (A) is explained. First in Step S4101S4102and S4103Processing in Step S401 of drawing 4 (A)S402and S403 and same processing are performeddecoding processing is made for the enciphered content read from the recording medium in the cipher-processing means 150 by thisand TS processing is made. The digital contents by which each processing was performed are supplied to input-and-output I/F120 via the bus 110.
[0340]Input-and-output I/F120 judges whether it is what the digital contents supplied there can copy later in Step S4104. That isthe contents are judged [that it can copy later and] when the information (copy control information) which expresses a copy control state to the digital contents supplied to input-and-output I/F120 like EMI or EMIfor example is not included.
[0341]When copy control informationsuch as EMIis included in the digital contents supplied to input-and-output I/F120 for exampleThereforewhen copy control informationsuch as EMIis recorded according to the standard of DTCP at the time of record of contents. Contents are judged [that it can copy later and] when copy control informationsuch as the EMI (recorded EMI (Recorded EMI))is Copy-freely. Contents are judged [that it cannot copy later and] when copy control informationsuch as EMIis No-more-copies.
[0342]Generally copy control informationsuch as recorded EMIis neither Copy-one-generation nor Copy-never. It is because the digital contents which EMI of Copy-one-generation is changed into No-more-copies at the time of recordand have EMI of Copy-never are not recorded on a recording medium. Howeverit is not this limitation when a rulesuch as "treating the copy control information of Copy-one-generation as No-more-copies although recorded without changing into No-more-copies"is decided in the system.
[0343]In Step S4104when contents are judged [that it can copy later and]it progresses to Step S4105and input-and-output I/F120 outputs the digital contents outsideand ends regeneration.
[0344]When contents are judged [that it cannot copy later and] in Step S4104progress to Step S4106 and input-and-output I/F120For exampleaccording to the standard of DTCPetc.it outputs outside in the form where digital contents are not copied to the digital contents laterand regeneration is ended.
[0345]Namelywhen copy control informationsuch as EMI recorded as mentioned abovefor exampleis No-more-copies (or) Although the copy control information of "Copy-one-generation is recorded in a systemwithout changing into No-more-copiesThe rule of treating as No-more-copies" is decidedand when copy control informationsuch as EMI recorded under the conditionsis Copy-one-generationas

for contentsthe copy beyond it is not allowed.
[0346]For this reasoninput-and-output I/F120 attests mutually between a partner's devices according to the standard of DTCPwhen a partner is a just deviceenciphers digital contents (when it is a device based on the standard of DTCP here)and outputs them outside.
[0347]Nextwhen reproducing the contents recorded on the recording medium and outputting outside as analog contentregeneration according to the flow chart of drawing 45 (B) is performed. Processing of drawing 45 (B) is explained. In Steps S4111 thru/or S4115processing in Steps S421 thru/or S425 of drawing 4 (B) and same processing are performed. That isread-out of enciphered contentdecoding processingTS processingMPEG decodingand D/A conversion are performed. The analog content obtained by this is received by input-and-output I/F140.
[0348]Input-and-output I/F140 judges whether it is what the contents supplied there can copy later in Step S4116. That isthe contents are judged [that it can copy later and] when copy control informationsuch as EMIis not recorded on the contents currently recorded together for example.
[0349]Contents are judged [that it can copy later and]when copy control informationsuch as EMIis recordedfor example according to the standard of DTCP at the time of record of contents and the information is Copy-freely.
[0350]When copy control informationsuch as EMIis No-more-copiesin a systemrecord the copy control information of "Copy-one-generationwithout changing into No-more-copiesbut. The rule of treating as No-more-copies" is decidedand contents are judged [that it cannot copy later and] when copy control informationsuch as EMI recorded under the conditionsis Copy-one-generation.
[0351]When a CGMS-A signal is included in the analog content supplied to input-and-outout I/F140 for exampleThereforeanalog content is judged [that it can copy later and]when a CGMS-A signal is recorded with the contents at the time of record of contents and the CGMS-A signal is Copy-freely. Analog content is judged [that it cannot copy later and] when a CGMS-A signal is Copy-never.
[0352]In Step S4116when contents are judged [that it can copy later and]it progresses to Step S4117and input-and-output I/F140 outputs outside the analog signal supplied there as it isand ends regeneration.
[0353]In Step S4116when contents are judged [that it cannot copy later and]it progresses to Step S4118and input-and-output I/F140 is outputted outside in the form where analog content is not copied to the analog content laterand ends regeneration.
[0354]Namelywhen copy control informationsuch as EMI recorded as mentioned abovefor exampleis No-more-copies (or) Although the copy control information of "Copy-one-generation is recorded in a systemwithout changing into No-more-copiesThe rule of treating as No-more-copies" is decidedand when copy control informationsuch as EMI recorded under the conditionsis Copy-one-generationas for contentsthe copy beyond it is not allowed.
[0355]For this reasoninput-and-output I/F140 adds the GCMS-A signal with

which a macro vision signal and Copy-never are expressed for analog content at itfor exampleand outputs it outside. For examplealso when the recorded CGMS-A signal is Copy-neveras for contentsthe copy beyond it is not allowed. For this reasoninput-and-output I/F4 changes a CGMS-A signal into Copy-neverand it outputs t outside with analog content.

[0356]As mentioned aboveit becomes possible by performing record reproduction of contents to prevent the copy (illegal copy) besides the range which contents were allowed from being performedperforming copy control of contents.

[0357][Composition of a data processing means] Software can also perform as well as in addition performing a series of processings mentioned above by hardware. That isit is also possible tohave composition performed by making a general-purpose computer and the microcomputer of one chip execute a program for examplealthough the cipher-processing means 150 can also be constituted as encryption/decoding LSI. TS processing means 300 can perform processing with software similarly. When software performs a series of processingsthe program which constitutes the software is installed in a general-purpose computerthe microcomputer of one chipetc. Drawing 46 shows the example of composition of the 1 embodiment of the computer by which the program which performs a series of processings mentioned above is installed.

[0358]A program is recordable on hard disk [as a recording medium] 4205and ROM4203 built in the computer beforehand. A program Or a floppy (registered trademark) diskCD-ROM (Compact Disc Read Only Memory)It is temporarily or permanently storable in the removable recording media 4210such as MO (Magneto optical) diskDVD (Digital Versatile Disc)a magnetic diskand semiconductor memory (record). Such a removable recording medium 4210 can be provided as what is called a software package.

[0359]Install a program in a computer from the removable recording medium 4210 which was mentioned aboveand also via the artificial satellite for the digital satellite broadcasting from a download siteVia networks [**** / transmitting to a computer on radio]such as LAN (Local AreaNetwork) and the InternetIt transmits to a computer with a cableand in a computerit can receive in the communications department 4208 and the program transmitted by making it such can be installed on the hard disk 4205 to build in.

[0360]The computer contains CPU(Central Processing Unit) 4202. The input/output interface 4211 is connected to CPU4202 via the bus 4201. CPU4202 via the input/output interface 4210 by a user. If instructions are inputted by operating the input part 4207 which comprises a keyboarda mouseetc.according to itthe program stored in ROM(Read Only Memory) 4203 will be executed.

[0361]Or a program by which CPU4202 is stored in the hard disk 4205A program which was transmitted from the satellite or the networkwas received in the communications department 4208and was installed on the hard disk 4205Or the program which was read from the removable recording medium 4210 with which

the drive 4209 was equippedand was installed on the hard disk 4205 is loaded to RAM(Random Access Memory) 4204and is executed.
[0362]TherebyCPU4202 performs processing performed by the composition of the block diagram according to the flow chart mentioned above processed or mentioned above. CPU4202 the processing result and via the input/output interface 4211 if neededIt is made to record on an output or the transmission from the communications department 4208and also the hard disk 4205 from the outputting part 4206 which comprises LCD (Liquid CryStal Display)a loudspeakeretc.
[0363]The processing step which describes the program for making various kinds of processings perform to a computer in this Description hereIt is not necessary to necessarily process to a time series in accordance with the order indicated as a flow chartand a parallel target or the processing (for exampleparallel processing or processing by an object) performed individually is also included.
[0364]A program may be processed by the computer of 1 and distributed processing may be carried out by two or more computers. A program may be transmitted to a distant computer and may be executed.
[0365]Although this embodiment explained as a center the example which constitutes the block which performs encryption/decoding of contents from encryption/decoding LSI of one chipThe block which performs encryption/decoding of contents can also be realized as one software module which CPU170 shown in drawing 1 and drawing 2 performsfor example. It is possible similarly to also realize processing of TS processing means 300 as one software module which CPU170 performs.
[0366][The manufacturing installation of a recording medium and method] Nextthe information-recording-medium manufacturing installation and method of this invention of manufacturing the information recording medium of this invention mentioned above are explained.
[0367]In drawing 47manufacture a recording mediumand to a recording medium Disk ID (Disk ID)Validation key blocks: The outline composition of the disk manufacturing installation which records EKB (Enabling Key Block) and the enciphered master keyor the enciphered medium key is shown.
[0368]As opposed to the information recording medium already assembled by the assembly process which the disk manufacturing installation shown in this drawing 47 does not illustrateDisk ID (Disk ID)validation key-blocks:EKB (Enabling Key Block) and the enciphered master keyor the enciphered medium key is recordedand the above-mentioned confidential information is recorded. The pre (pre-recording) record generation information (Generation#n) of a master key is also recorded collectively if needed.
[0369]the disk manufacturing installation 4300 -- disk ID (Disk ID) and validation key-blocks:EKB (Enabling Key Block) -- andThe memory measure of the memory 4302 or others which stores beforehand the enciphered master key or the enciphered medium keyIt has recording-medium I/F4303 which performs the reading and writing to the recording medium 4350input-and-output I/F4304 used

as I/F w th other devicesthe control section 4301 which controls themand the bus 4305 which connects these.
[0370]Although the memory 4302 and recording-medium I/F4304 give the example built in the manufacturing installation concerned in the composition of drawing 47the memory 4302 and recording-medium I/F4303 may be external things.
[0371]above-mentioned disk ID (Disk ID) and validation key-blocks:EKB (Enabling KeyBlock) -- andConfidential informationsuch as an enciphered master key or an enciphered medium keyand stamper IDPre (pre-recording) record generation information (Generation#n) of a master key is published by the identifier administration which does not illustratefor examplethe key issue centeretc.
It is befcrehand stored in above built-in or an external memory.

[0372]Disk ID stored in the above-mentioned memory 4302 (Disk ID)Validation key blocks: Confidential information and the enciphered master keyor the medium keys which were encipheredsuch as EKB (Enabling Key Block) and stamper IDare recorded on a recording medium via recording-medium I/F4303 under control of the control section 4301. It records also about the pre (pre-recording) record generation information (Generation#n) of a master key if needed.
[0373]For examplethe above-mentioned writing of confidential information and the [reproduction] column explained confidential informationsuch as stamper IDit is the data generated according to the confidential information generation processing means with the composition of drawing 25drawing 27etc.
According to each compositionthe data conversion about confidential informationsuch as stamper IDis madeand the translation data obtained as the result is written in a recording medium.

[0374]disk ID (Disk ID) and validation key-blocks:EKB (Enabling KeyBlock) -- andThe enciphered master key or the enciphered medium keyand the pre (pre-recording) record generation information (Generation#n) of a master keyIt is also possible for what it not only uses what is beforehand stored in the memory 4302 as mentioned abovebut has been sent from the key issue centerfor example via input-and-output I/F4304 to come to hand.
[0375]As a recording-medium manufacturing method of this inventionin drawing 48manufacture the above-mentioned recording mediumand. as opposed to a recording medium -- disk ID (Disk ID) and validation key-blocks:EKB (Enabling Key Block) -- andThe flow of the manufacturing process in the enciphered master key or the enciphered medium keyand the recording-medium manufacturing method which records the pre (pre-recording) record generation information (Generation#n) of a master key is shown.
[0376]In drawing 48various recording mediasuch as DVD and CDare first assembled as a manufacturing process of Step S4401 by a recording-medium manufacturing method by the publicly known assembly process which is not illustrated.
[0377]Nextas a manufacturing process of Step S4402 by the recording-medium

manufacturing installation of drawing 47. To the manufactured recording mediumdisk ID (Disk ID)stamper ID as confidential information (Stamper ID)Validation key blocks: Perform recording processing of EKB (Enabling Key Block) and the enciphered master keyor the enciphered medium key. The pre (pre-recording) record generation information (Generation#n) of a master key is recorded if needed.

[0378]By the above disk manufacturing process processa recording mediumWhere disk ID (Disk ID)validation key-blocks:EKB (Enabling Key Block) and the enciphered master key or the enciphered medium keyand stamper ID as confidential information are recordedit is shipped from a plant. After recording the pre (pre-recording) record generation information (Generation#n) of a master key if neededit is shipped from a plant.

[0379]Disk ID set up by recording as confidential information differing not only for stamper ID but for every diskIt may record as confidential information which differs for every contents and stores various identification datasuch as content ID to set up or a key for cipher processingand a cipher-processing key in a disk. In a recording and reproducing devicethe cipher-processing key of contents is generated with the application of such various confidential information.

[0380][Format of EKB] The example of a format of validation key blocks (EKB:Enabling Key Block) is shown in drawing 49. The version 4501 is an identifier which shows the version of validation key blocks (EKB:Enabling KeyBlock). The depth 4502 shows the hierarchy number of the hierarchy tree to the device of the distribution destination of validation key blocks (EKB:Enabling Key Block). The data pointer 4503 is a pointer in which the position of the data division in validation key blocks (EKB:Enabling Key Block) is shown.

It is a pointer which the tag pointer 4504 shows the position of a tag part toand the signature pointer 4505 shows the position of a signature.

The data division 4506 stores the data which enciphered the node key updatedfor example.

[0381]The tag part 4507 is a tag in which the physical relationship of the node key and leaf key which were stored in the data divisionand which were enciphered is shown. The grant rule of this tag is explained using drawing 50. Drawing 50 shows the example which sends the validation key blocks (EKB) previously explained by drawing 12 (A) as data. The data at this time comes to be shown in the table on the right of drawing 50. Let the address of the top node contained in the cryptographic key at this time be a top node address. In this casesince updating key K(t) R of the route key is containeda top node address serves as KR.

[0382]The data Enc (K(t) 0 and K (t) R) of the highest rung of a cryptographic key is in the position shown in the hierarchy tree on the left of drawing 50. Herethe following data is Enc (K (t) 00K(t)0).

It is in the position at the lower left of front data on a tree.

A tag is set upand 1 is set up when there is dataand there is nothing0 and. A tag is set up as {a left (L) tag and a right (R) tag}. Since there is data in the left of the data Enc (K(t) 0 and K (t) R) of the highest rung and there is no data in L tag =0

and the rightit is set to R tag =1. Hereaftera tag is set as all the data and the data row shown in drawing 50 (c) and a tag sequence are constituted.
[0383]It is preferred to use depth-first (depth first) either the width priority (breadth first) processing in which the cross direction of the same stage is processed previously or processing which processes a depth direction previously as turn of node processing of a tree.
[0384]It returns to drawing 49 and an EKB format is explained further. For examplethe signature (Signature) published validation key blocks (EKB)it is an electronic signature which a lock management centercontents ROBAIDAa settlement-of-accounts organizationetc. perform. It checks that the devices which received EKB are the validation key blocks (EKB) which the just validation key-blocks (EKB) publisher published by signature verification.
[0385]As mentioned aboveit has explained in detail about this inventionreferring to specific working example. Howeverit is obvious that a person skilled in the art can accomplish correction and substitution of this working example in the range which does not deviate from the gist of this invention. For exampleas mentioned aboveexplained the example which set to stamper ID confidential information of which the specific data writing processing stored in a disk and regeneration are required in working examplebut. It is possible to set up not only stamper ID but various identification datasuch as disk ID set up by differing for every diskcontent ID differed and set up for every contentsor a key for cipher processingand a cipher-processing key as confidential information stored in a disk. In working examplewith the gestalt of illustrationthis invention has been indicated and it should not be interpreted restrictively. In order to judge the gist of this inventionthe column of the Claims indicated at the beginning should be taken into consideration.
[0386]
[Effect of the Invention]As mentioned abovein the composition of this inventionits writing / the read-out method with difficult analysis beforehand to a recording medium. The signal of the confidential information which can be read was stored only with the special read methodand it had composition which makes the above-mentioned confidential information act on the contents encryption at the time of performing record or reproduction of contents of music dataimage dataetc. to this recording mediumor the encryption key for decoding processings. Thereforeonly in the just device which can perform the specific method of readinggeneration of reading of confidential information and the cipher-processing key of contents is attainedand it becomes possible to prevent effectively the contents playback in the device which cannot perform how to read confidential information.
[0387]In the composition of this inventionthe confidential information which can be read only with a special read methodIt is read with a just devicei.e.the device which can perform how to read confidential informationFor exampleit is the composition used for the key generation processing for contents cipher processing under secure protection in the cipher-processing part which performs generation of the encryption key which was mounted in LSI and protected highlyand

confidential information is not stored on the memory in which reading from the outside is possible. Thereforethere is no possibility of disclosure of confidential information and it becomes possible to prevent regeneration of inaccurate contents effectively.

[0388]According to the composition of this inventionby the key distribution configuration of tree (Thurs.) structure. The master key and medium key which transmitted a master key and the update information of the medium key with validation key blocks (EKB)and transmittedSince it had composition which performs contents encryption or encryption key generation processing for decoding processings based on the confidential information which can be read only by the special technique to readUse of contents is attained only with the just device which could perform the special method of reading about confidential information and to which the key was distributed by the key distribution configuration of the tree structure.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the example of composition of the Information Storage Division playback equipment of this invention (the 1).

[Drawing 2]It is a block diagram showing the example of composition of the Information Storage Division playback equipment of this invention (the 2).

[Drawing 3]It is a figure showing the Data Recording Sub-Division process flow of the Information Storage Division playback equipment of this invention.

[Drawing 4]It is a figure showing the data reproduction process flow of the Information Storage Division playback equipment of this invention.

[Drawing 5]It is a figure explaining the data format processed in the Information Storage Division playback equipment of this invention.

[Drawing 6]It is a block diagram showing the composition of the transport stream (TS) processing means in the Information Storage Division playback equipment of this invention.

[Drawing 7]It is a figure explaining the composition of the transport stream processed in the Information Storage Division playback equipment of this invention.

[Drawing 8]It is a block diagram showing the composition of the transport stream (TS) processing means in the Information Storage Division playback equipment of this invention.

[Drawing 9]It is a block diagram showing the composition of the transport stream (TS) processing means in the Information Storage Division playback equipment of this invention.

[Drawing 10]It is a figure showing the example of composition of the block data as additional information of block data processed in the Information Storage Division playback equipment of this invention.

[Drawing 11]It is a tree lineblock diagram explaining the encryption processing of

keyssuch as a master key and a medium keyto the Information Storage Division playback equipment of this invention.
[Drawing 12]It is a figure showing the example of the validation key blocks (EKB) used for the distribution of keyssuch as a master key and a medium keyto the Information Storage Division playback equipment of this invention.
[Drawing 13]It is a figure showing the example of distribution which uses the validation key blocks (EKB) of the master key in the Information Storage Division playback equipment of this inventionand the example of decoding processing.
[Drawing 14]It is a figure showing the decoding processing flow which uses the validation key blocks (EKB) of the master key in the Information Storage Division playback equipment of this invention.
[Drawing 15]It is a figure showing the generation comparison processing flow of the master key in the contents recording processing in the Information Storage Division playback equipment of this invention.
[Drawing 16]In the Information Storage Division playback equipment of this inventionit is a block diagram (the 1) explaining the encryption processing at the time of the Data Recording Sub-Division processing.
[Drawing 17]In the Information Storage Division playback equipment of this inventionit is a block diagram (the 2) explaining the encryption processing at the time of the Data Recording Sub-Division processing.
[Drawing 18]In the Information Storage Division playback equipment of this inventionit is a flow chart explaining the Data Recording Sub-Division processing.
[Drawing 19]It is a figure explaining the example of generation of the disk inherent key in the Information Storage Division playback equipment of this invention.
[Drawing 20]It is a figure showing the EMI storing position (5CDTCP standard) in transmission 1394 packet processed in the Information Storage Division playback equipment of this invention.
[Drawing 21]It is a flow chart explaining the process of determining whether performing contents recording in the Information Storage Division playback equipment of this invention by a data analysis recording method (Cognizant Mode)or perform by data a non-analyzing recording method (Non-Cognizant Mode).
[Drawing 22]In the Information Storage Division playback equipment of this inventionit is a figure showing the example of generation processing of the title inherent key at the time of Data Recording Sub-Division.
[Drawing 23]It is a figure explaining the generation method of the block key in the Information Storage Division playback equipment of this invention.
[Drawing 24]It is a figure showing the generation processing flow of the title inherent key in the Information Storage Division playback equipment of this invention.
[Drawing 25]It is a figure showing the modulation circuit applied to the recording processing of confidential informationsuch as stamper ID in the Information Storage Division playback equipment of this invention.
[Drawing 26]It is a figure showing the confidential information decoding processing circuit applied to regeneration of confidential informationsuch as stamper ID

shown in drawing 25.
[Drawing 27]It is a figure showing the example of record composition of confidential informationsuch as stamper ID in the Information Storage Division playback equipment of this invention.
[Drawing 28]It is a figure showing the confidential information decoding processing circuit applied to regeneration of confidential informationsuch as stamper ID shown in drawing 27.
[Drawing 29]It is a figure showing the example of recording and reproducing device composition which stored only the key for data analysis record in the Information Storage Division playback equipment of this invention.
[Drawing 30]It is a figure showing the example of recording and reproducing device composition which stored only the key for data non-analyzing record in the Information Storage Division playback equipment of this invention.
[Drawing 31]In the Information Storage Division playback equipment of this inventionit is a block diagram explaining the contents data decryption processing at the time of data reproduction processing.
[Drawing 32]In the Information Storage Division playback equipment of this inventionit is a flow chart explaining data reproduction processing.
[Drawing 33]In the Information Storage Division playback equipment of this inventionit is a flow chart which shows the details of the refreshable system decisior processing in data reproduction processing.
[Drawing 34]In the Information Storage Division playback equipment of this inventionit is a figure showing the generation processing flow of the title inherent key at the time of data reproduction.
[Drawing 35]It is a figure showing the example of distribution which uses the validation key blocks (EKB) of the medium key in the Information Storage Division playback equipment of this inventionand the example of decoding processing.
[Drawing 36]It is a figure showing the decoding processing flow which uses the validation key blocks (EKB) of the medium key in the Information Storage Division playback equipment of this invention.
[Drawing 37]It is a figure showing the contents recording process flow which uses the medium key in the Information Storage Division playback equipment of this invention.
[Drawing 38]In the Information Storage Division playback equipment of this inventionit is a block diagram (the 1) explaining the encryption processing at the time of the Data Recording Sub-Division processing which uses a medium key.
[Drawing 39]In the Information Storage Division playback equipment of this inventionit is a block diagram (the 2) explaining the encryption processing at the time of the Data Recording Sub-Division processing which uses a medium key.
[Drawing 40]In the Information Storage Division playback equipment of this inventionit is a flow chart explaining the Data Recording Sub-Division processing which uses a medium key.
[Drawing 41]In the Information Storage Division playback equipment of this inventionit is a block diagram explaining the encryption processing at the time of

the data reproduction processing which uses a medium key.
[Drawing 42]In the Information Storage Division playback equipment of this inventionit is a flow chart explaining the data reproduction processing which uses a medium key.
[Drawing 43]In the Information Storage Division playback equipment of this inventionit is a flow chart which shows the details of the refreshable nature decision processing in the data reproduction processing which uses a medium key.
[Drawing 44]It is a flow chart explaining the copy control processing at the time of the Data Recording Sub-Division processing in the Information Storage Division playback equipment of this invention.
[Drawing 45]It is a flow chart explaining the copy control processing at the time of the data reproduction processing in the Information Storage Division playback equipment of this invention.
[Drawing 46]In the Information Storage Division playback equipment of this inventionit is a block diagram showing the processing means composition in the case of performing data processing with software.
[Drawing 47]It is a block diagram showing the composition of the manufacturing installat on which manufactures the information recording medium used in the Information Storage Division playback equipment of this invention.
[Drawing 48]It is a figure showing the process flow of a manufacturing process which manufactures the information recording medium used in the Information Storage Division playback equipment of this invention.
[Drawing 49]It is a figure showing the example of a format of the validation key blocks (EKB) used in the Information Storage Division playback equipment of this invention.
[Drawing 50]It is a figure explaining the composition of the tag of the validation key blocks (EKB) used in the Information Storage Division playback equipment of this invention.
[Description of Notations]
100200 Recording and reproducing device
110 Bus
120 Input-and-output I/F
130 MPEG codec
140 Input-and-output I/F
141 A/Da D/A converter
150 Cipher-processing means
160 ROM
170 CPU
180 Memory
190 Drive
195 Recording medium
210 Recording-medium I/F
300 TS processing means
500 Confidential information decode processing means

600607 Terminal
602 Bit stream purser
603 PLL
604 Time stamp generation circuit
605 Block seed additional circuit
606 Smoothing buffer
800806 Terminal
801 Block seed separation circuits
802 Output controlling circuit
803 Comparator
804 Timing generating circuit
805 27 MHz clocks
901904913 Terminal
902 MPEG video encoder
903 Video stream buffer
905 MPEG audio encoder
906 Audio stream buffer
908 Multiplexing scheduler
909 Transport packet coding equipment
910 Arrival-time-stamps calculating means
911 Block seed additional circuit
912 Smoothing buffer
976 Switch
1041 PLL circuit
1042 Timing generator
1043 Alignment pattern generation circuit
1045 M sequence generation circuit
1046 Arithmetic circuit
1047 Random number generation circuit
1048 Data selector
1049 Data selector
1081 PLL circuit
1082 Synchronization detecting circuit
1083 M sequence generation circuit
1084 Multiplication circuit
1085 Integration circuit
1086 Decision circuit
1160 PLL circuit
1161 Synchronization detecting circuit
1162 Timing generator
1163 Flip-flop
1164 Maximum detector circuit
1165 Parallel serial conversion circuit
4202 CPU

4203 ROM
4204 RAM
4205 Hard disk
4206 Outputting part
4207 Input part
4208 Communications department
4209 Drive
4210 Removable recording medium
4211 Input/output interface
4300 Disk manufacturing installation
4301 Control section
4302 Memory
4303 Recording-medium I/F
4304 Input-and-output I/F
4305 Bus
4350 Recording medium
4501 Version
4502 Depth
4503 Data pointer
4504 Tag pointer
4505 Signature pointer
4506 Data division
4507 Tag part
4508 Signature